NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BANDWIDTH MANAGEMENT IN RESOURCE CONSTRAINED NETWORKS

by

Christopher T. Schrock

March 2012

Thesis Advisor:	William J. Welch
Second Reader:	Douglas J. MacKinnon

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Bandwidth Management in Resource Constrained Networks		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Christopher T. Schrock			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

Hastily Formed Networks (HFNs) are typically deployed in resource constrained environments. Clients operating within HFNs have inadvertently utilized excessive bandwidth without user interaction. Our research focuses on managing bandwidth usage in resource constrained networks through the use of DNS Tampering, a method of content filtering. We evaluate two operating systems, Windows XP and Windows 7, and analyze how it may be possible to limit operating system updates utilizing DNS Tampering. We then explore how it may be possible to implement this technique utilizing equipment available for an HFN. Through our efforts, we develop and set forth specific methodologies that can provide the opportunity to limit bandwidth usage for specific applications in resource constrained networks.

14. SUBJECT TERMS Content Filtering, Hastily Formed Network (HFN), Network Management, Traffic Management, Bandwidth Management, Domain Name System (DNS), Domain Name Service (DNS)			**15. NUMBER OF PAGES** 143
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 8–98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

BANDWIDTH MANAGEMENT IN RESOURCE CONSTRAINED NETWORKS

Christopher T. Schrock
Lieutenant, United States Navy
A.S., Amarillo College, 1997
B.B.A., West Texas A&M University, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2012

Author: Christopher T. Schrock

Approved by: William J. Welch
Thesis Advisor

Douglas J. MacKinnon, PhD
Second Reader

Dan Boger, PhD
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Hastily Formed Networks (HFNs) are typically deployed in resource constrained environments. Clients operating within HFNs have inadvertently utilized excessive bandwidth without user interaction. Our research focuses on managing bandwidth usage in resource constrained networks through the use of DNS Tampering, a method of content filtering. We evaluate two operating systems, Windows XP and Windows 7, and analyze how it may be possible to limit operating system updates utilizing DNS Tampering. We then explore how it may be possible to implement this technique utilizing equipment available for an HFN. Through our efforts, we develop and set forth specific methodologies that can provide the opportunity to limit bandwidth usage for specific applications in resource constrained networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BGAN	Broadband Global Access Network
DESRON	Destroyer Squadron
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GSA	U.S. Government Services Administration
HA/DR	Humanitarian Assistance/Disaster Relief
HFN	Hastily Formed Network
HTTP	Hypertext Transfer Protocol
IDP	Indigenous Displaced Personnel
IP	Internet Protocol
J6	Communications
JFMCC	Joint Forces Maritime Component Command
JTF	Joint Task Force
JUSMAGTHAI	Joint U.S. Military Advisory Group Thailand
KB	Kilobyte
MB	Megabyte
NAT	Network Address Translation
NGO	Non-Government Organization
NPS	Naval Postgraduate School
OSI	Open Systems Interconnection
QoS	Quality of Service
TCP	Transmission Control Protocol/Internet Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Networks
VSAT	Very Small Aperture Terminal
WAP	Wireless Access Point

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I could not have completed this thesis without the motivation from my wife, Claudia. You are the love of my life and I could not have made it to the end without your strength and dedication. Also, to my son, Andrew, and daughter, Morgan. You sacrificed countless hours throughout several months away from Daddy so that I may complete my thesis.

I want to thank my advisors, Mr. Joe Welch and Dr. Doug MacKinnon. Your insight and experience turned my seemingly random visions of a concept into a tangible research project and final product. Your time and attention ultimately culminated into a project of which I am proud.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND OF HFN

At the time of the December 26, 2004, Southeast Asia earthquake, a group of faculty and students from Naval Postgraduate School (NPS) were scheduled to conduct research on the use of wireless communications in border security in cooperation with the Royal Thai Armed Forces. In response to the earthquake and devastating tsunami which followed, the focus immediately shifted from technical research and demonstration to operational application in support of Humanitarian Assistance/Disaster Relief (HA/DR) (Steckler, 2010).

The team, in cooperation with the Royal Thai Armed Forces and the Joint U.S. Military Advisory Group Thailand (JUSMAGTHAI), utilized their wireless capabilities to support early responders in Takuapa, Thailand. The Buddhist Temple in Takuapa was being established as the largest morgue and grave registration site in Thailand in response to the tsunami. Researchers leveraged their Very Small Aperture Terminal (VSAT) to create an Internet backbone with a commercial satellite Internet provider. A meshed Wi-Fi cloud was connected, providing free and open Internet access around the temple to be used by anyone needing access to the Internet. A Wi-Fi bridge was established extending the reach of the Internet backbone approximately seven kilometers to the largest Indigenous Displaced Personnel (IDP) camp. An additional Wi-Fi mesh network was implemented at the camp providing an Internet cloud, accessible by nearly 800 individuals comprised of survivors and support personnel, including Non-Government Organizations (NGOs). In all, a Hastily Formed Network (HFN) was supported for approximately five months and included several trips to the area to improve, enhance, and learn from the experience (Steckler, 2010).

Following the tsunami, the NPS group reorganized and began a predominate focus on HA/DR, officially establishing NPS's HFN Center. Approximately three months after concluding work in Thailand, "one of the

strongest storms to impact the coast of the United States during the last 100 years" struck the U.S. Gulf Coast (National Climatic Data Center, 2005). Hurricane Katrina struck the U.S. Gulf Coast on August 29, 2005 and NPS's HFN Center was called upon to support recovery missions in the Gulf area. The HFN group, partnered with commercial wireless vendors, deployed to Bay St. Louis and Waveland, Mississippi. Their objective was to provide immediate, sustainable, and freely accessible Internet access for the communities "for all early responders, victims' families, and government (local and federal)" through the use of two VSATs and mesh Wi-Fi networks. Supporting Katrina operations in the gulf solidified the viability, validity, and necessity of NPS's HFN Center. Throughout the next five years, the group of researchers upgraded their wireless equipment and capabilities, began conducting research, and participated in multi-national and U.S. Government exercises focused on disaster communications and interoperability (Naval Postgraduate School and the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD-NII), 2011).

B. HAITI EARTHQUAKE

NPS's HFN Center deployed on January 18, 2010, in response to the devastating earthquake occurring in Haiti one week prior. The team's primary task was providing advice and support, to include communications capability, to Destroyer Squadron (DESRON) 40 onboard the USNS Comfort, one of two active U.S. Navy hospital ships. As similar to the previous two HA/DR operations, students and faculty from NPS, known as NPS HFN TEAM HAITI, deployed to the area and prepared to establish communications networks in support of recovery operations. Approximately two weeks after deployment, the team's support was redirected from DESRON 40 to the larger Joint Task Force Haiti (JTF Haiti). Specifically, the team was "to bring to bear (their) experience with ad hoc rapidly deployed networks in austere environments" (Steckler, 2010).

One of the methods utilized for providing communications access was through the use of BGAN (Broadband Global Access Network) service. BGANs are “highly portable terminals” which “can easily fit in your backpack or be mounted onto vehicles for comms-on-the-move” (Inmarsat, 2012).

The NPS team deployed to Haiti with several Inmarsat commercial BGAN units capable of providing data rates of up to 400 kbps. The BGANs were utilized in a variety of methods including videoconferencing, web access, text chatting, and voice communications. As BGAN usage increased across the area in the first weeks of the response, the NPS group noticed significant service availability issues. Inmarsat acknowledged that there were simply too many subscribers attempting to utilize too much bandwidth. However, it was expected that as larger, more permanent services were established in the area, BGAN demand would decrease and normal operations and availability would resume (Steckler, 2010).

While BGAN services are exceptionally versatile and extremely beneficial, there is a generally high cost associated with the service. BGAN service is normally billed on a usage based rather than a flat rate service. Services such as video, voice, or large imagery can quickly consume large amounts of bandwidth and incur significant costs. Given the relatively high costs associated with BGAN service, the limited bandwidth should be managed and protected (Nelson, Steckler, & Stamberger, 2011).

The high costs associated with BGAN service manifested itself first hand to the NPS HFN team during Haiti. A single BGAN unit utilized over $2,000 of service in less than 36 hours. The initial fear was that the connection was somehow maliciously utilized and hijacked. Cooperative forensics between Inmarsat and NPS HFN personnel determined that the true cause of the sudden surge in usage was due to the BGAN and one laptop being inadvertently powered on and connected. During that period, operating system updates ran in

the background on the laptop continuously utilizing the network connection to send and receive traffic. The immediate response was to ensure system updates were disabled (Steckler, 2010).

After discovering the inadvertent error, the HFN team was contacted by the Joint Forces Maritime Component Command (JFMCC) J6 (Communications). The JFMCC reported that a U.S. Coast Guard detachment was incurring an exceptionally large bill for BGAN service, at one point exceeding $5,000 per day. The HFN team passed along the lessons learned concerning laptops configured to perform automatic updates (Steckler, 2010).

C. POSSIBLE METHODS TO MITIGATE INADVERTENT BANDWIDTH CONSUMPTION

The primary method to mitigate inadvertent high consumption of bandwidth when utilizing BGAN is user education and training. Understanding the high costs associated with the service as well as how computers utilize network connections is invaluable in properly managing resources. While the former is rather easy to articulate, that BGANs are providers of data and data costs money, the latter is beyond what most users understand.

BGAN services are available in a variety of pricing structures including monthly and annual recurring contracts as well pre-paid per megabyte (MB) of usage. If a BGAN is utilized in response to a disaster, it most likely is being activated and funded for that immediate purpose. Therefore, the data services are most likely being funded through pre-paid service agreements on a per-use basis.

A perspective on the cost of BGAN service is available by looking at the prices available through the GSA (U.S. Government Services Administration) Schedules. SatCom Global is a commercial provider of BGAN services and offers a variety of pricing options. Most of their per-use packages bill services in “units” where each megabyte of data requires eight units. The 5,000 unit pre-paid

plan provides 625MB of data at a cost of $3,989.70. This equates to $6.38 per MB. Short-term three month post-paid plans are available for $5.45 per MB (SatCom Global, 2012).

While we can articulate the actual costs of data, most users will have no concept of how much data is being utilized. If the high costs associated with BGANs are difficult for users to conceptualize, explaining to users how computers consume network traffic, even when left idle, will prove very difficult. While users of BGANs should be encouraged to understand the applications they have installed and how they devour the available Internet bandwidth, it is unreasonable to expect early responders to be capable of managing or controlling all of the applications installed on the computers they are provided for use in the field. Instead, alternative means must be explored. Technological methods for controlling and managing bandwidth consumption can be broken into two categories: limiting access to bandwidth and limiting how bandwidth can be utilized.

Limiting access to bandwidth as a method of controlling bandwidth consumption is used on a daily basis in hotels and Internet cafés. These providers of Internet services control access to their network through some sort of registration and usage monitoring service. This method does not seek to limit what a user may do with their access, it only limits who may utilized the service and how much service may be used (Hotel Internet Services [HIS], 2011).

The second category for controlling bandwidth is concerned with what the Internet service is being utilized for (the content being accessed) and less concerned with who, or how much, it is being used. This method is routinely referred to as content filtering and can limit access to specific content while allowing other traffic to pass uninhibited. Content filtering can be performed through a variety of techniques. This research will discuss several of these methods and evaluate the effectiveness of a particular method of content filtering as a method of limiting bandwidth in resource constrained networks.

D. OUTLINE OF THESIS

In Chapter II, we will review the concepts of Internet communications and discuss possible methods of content filtering. We will examine the implications associated with various methods of content filtering.

In Chapter III, we will introduce and describe our testing methodology for evaluating the effectiveness of Domain Name System (DNS) Tampering in bandwidth management. We will discuss the setup of our experiments and the steps involved in building the test bed. We will also introduce the supporting applications and technologies required to complete our experiments.

In Chapters IV and V, we will present our results and conclusions respectively. We will then discuss further research that can be done further refine this method, additional alternative methods to manage bandwidth in resource constrained networks, and provide a recommendation for implementation of DNS Tampering for use in HFNs.

II. CONTENT FILTERING

A. BACKGROUND

Content filtering is the process of interrupting a network connection for a specific purpose. Access to the Internet may be filtered for a variety of reasons including:

- Preventing access to content deemed inappropriate or unacceptable for the user (pornography).
- Blocking content harmful or damaging to the network (mal-ware).
- Ensuring only select information is available (kiosk).

There are as many different ways as there are reasons to accomplish content filtering. Each method may be evaluated based on a variety of factors including access to and control of the network, the desired reliability, and the ultimate purpose of filtering. The factors important in selecting a particular method of content filtering will be based on each user's needs.

Content filtering is accomplished through combinations of hardware and software. Each method of content filtering targets the communication in a specific manner resulting in some sort of interruption. Since the Internet relies on Transmission Control Protocol/Internet Protocol (TCP/IP) for all end-to-end communications, we will explore TCP/IP filtering (Socolofsky & Kale, 1991). The four primary types of TCP/IP filtering are TCP/IP Header Filtering, TCP/IP Content Filtering, DNS Tampering, and Hypertext Transfer Protocol (HTTP) Proxy Filtering (Murdoch & Anderson, 2008).

Each method of filtering affords different results. Driving factors in selecting a filtering method include available capability, desired reliability, and the desired results of the filtering. Available capability includes considerations such as access to or control of the network being utilized and the financial means to implement solutions. Reliability extends beyond simply the ability to limit access

to specific content through ordinary access. Reliability also considers the amount of overblocking (false positives) as well as effectiveness against those who purposefully attempt to bypass the filtering.

B. NORMAL TCP/IP COMMUNICATIONS

The Internet is a “complex network WAN that connects LANs and clients around the globe” (Dean, 2009). These connections are facilitated and managed through a suite of protocols known as TCP/IP. Most communications are accomplished through a multistep process which begins when the user requests a resource on the Internet by typing in a Uniform Resource Locator (URL) into a web browser. The user’s workstation sends the requested URL to a DNS server to be resolved to an IP (Internet Protocol) address. The response to the DNS query, in the form of an IP, is returned to the user’s workstation. The user’s workstation utilizes the IP address to contact the server on the Internet and request information. Finally, the server responds to the request (Socolofsky & Kale, 1991). This process is illustrated in Figure 1. While most users interact with the Internet through the use of URLs, the actual communications take place via the IP address (Kurose & Ross, 2009).

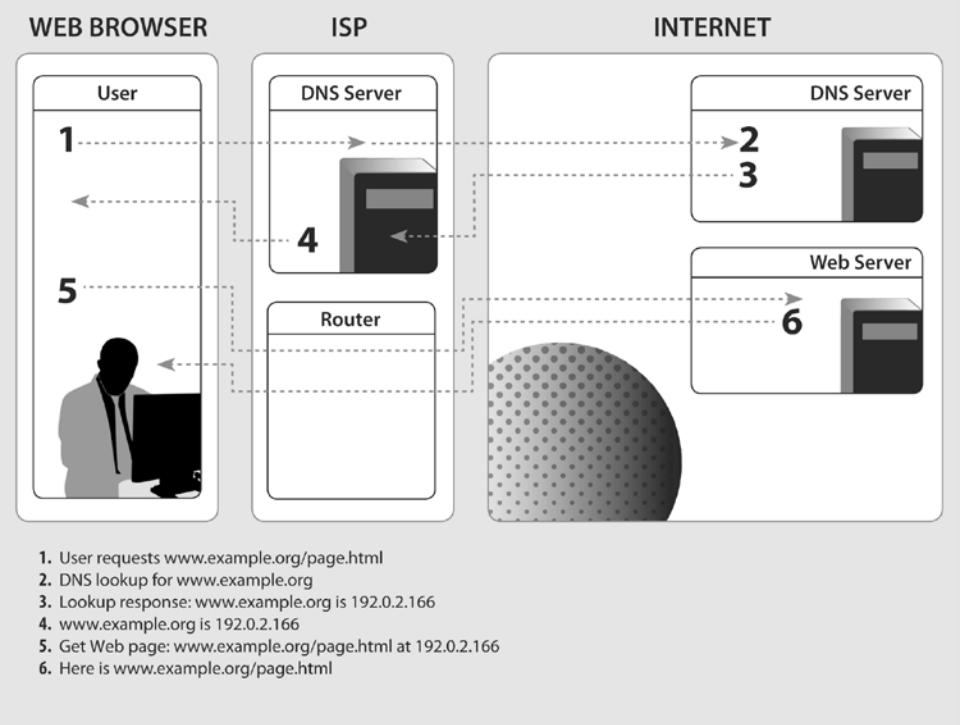

Figure 1 Normal TCP/IP Communication (After Murdoch & Anderson, 2008)

C. TCP/IP HEADER FILTERING

The TCP/IP header contains information including the source IP, source port number, destination IP, and destination port number. Routers connect networks with different addresses and transfer, or route, traffic between them. Depending on the network topology, TCP/IP communication will most likely traverse a series of routers. Routers utilize the information contained in the TCP/IP header to determine how and where to route the message or traffic (Dean, 2009) (Kurose & Ross, 2009).

TCP/IP Header Filtering relies on routers to analyze normal TCP/IP communications. Based on the information contained in the TCP/IP header, the router determines which traffic to allow, or pass, and which traffic to interrupt. While the determination may be based on any number of fields within the TCP/IP header, the decision is usually based on the destination IP resulting in packets intended for a specific recipient to be dropped or blocked, known as *blacklisting*. Further refinement may be made by blocking traffic destined only for specific

ports or only originating from specific IP addresses (Murdoch & Anderson, 2008). This process is illustrated in Figure 2. However, the implications of TCP/IP Header Filtering may not always be summarized this simply.

While TCP/IP Header Filtering results in blocking all undesired traffic past the router, this method is relatively coarse in nature. Multiple resources on the Internet may share a single IP address. When the single IP address is blocked, all resources sharing that address will also be unavailable. The unintended consequence may be overblocking, a situation in which legitimate resources are inadvertently disallowed, based on sharing an IP address of a blacklisted service (Edelman, 2003).

Additionally, since IP addresses may not be static and are subject to change, TCP/IP Header Filtering requires frequent maintenance and updating of deny lists. The blocked IP address of an undesired resource on the Internet may change to a new address which is not on our denied list. Without proper maintenance, access to the resource may no longer be restricted resulting in *underblocking*, a situation in which information is incorrectly allowed which should otherwise be blocked. Further, an otherwise innocent resource on the Internet may be blocked when assigned to the previously blacklisted address (Edelman, 2003).

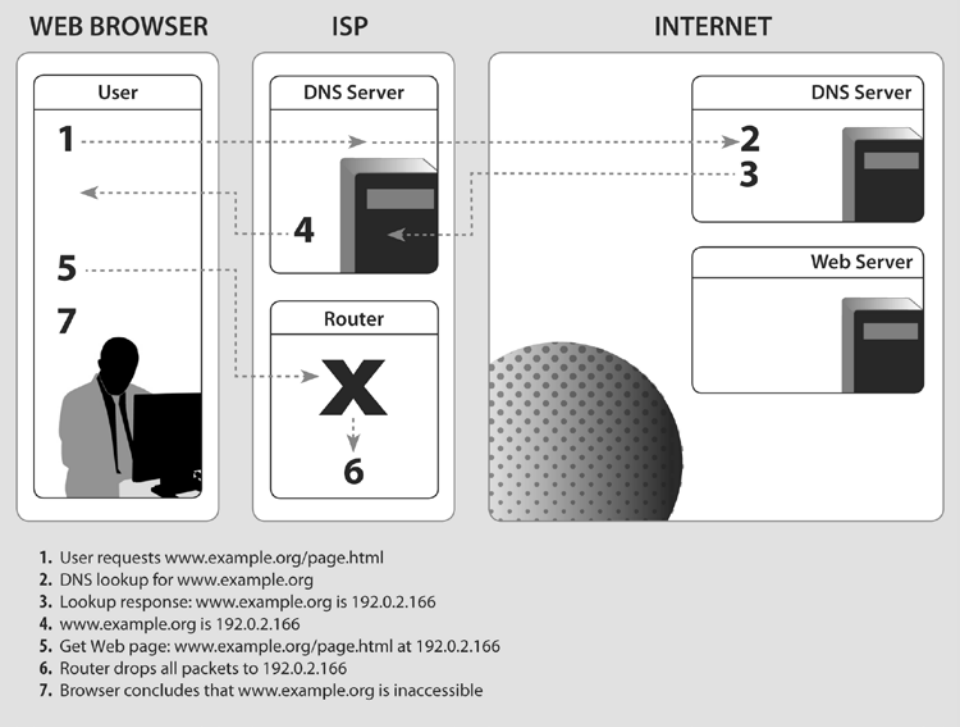

Figure 2 TCP/IP Header Filtering (After Murdoch & Anderson, 2008)

D. TCP/IP CONTENT FILTERING

TCP/IP Content Filtering does not rely on known lists of IP addresses to enable blocking. Rather TCP/IP Content Filtering inspects the actual content, or payload, of TCP/IP packets looking for banned content (Murdoch & Anderson, 2008). This content is usually in the form of keywords or phrases but may also consist of binary data. TCP/IP Content Filtering is best understood through an example. If the desired outcome is to block all traffic dealing with boating, a keyword list of ship, boat, raft, watercraft, etc., could be generated. Packets would be inspected for these keywords, and packets found to contain any of these keywords would be discarded and the communication, or message traffic, interrupted.

Like TCP/IP Header Filtering, TCP/IP Content Filtering is subject to *overblocking* and *underblocking*. Based on the previous example of denying nautical related traffic, one of our keywords is “ship.” When a request is made to

"ship a package," this legitimate traffic would be disallowed based on the request containing the keyword "ship." Conversely, a request regarding "ships on the sea" would be allowed since the word "ships" does not match our keyword of "ship." Similarly, a request containing "water vessel" or "kayak" would also be allowed. To compensate for these simple examples as well as the very nature of how TCP/IP operates, TCP/IP Content Filtering rules must become very complex and robust (Murdoch & Anderson, 2008).

Partially what permits TCP/IP to be so reliable, resilient, and efficient is that most messages are not isolated to a single TCP/IP packet. Instead, the protocol is designed to allow content to be split across multiple packets (Socolofsky & Kale, 1991). This technical aspect of TCP/IP frequently results in denied content being broken into multiple pieces and spread throughout multiple packets. When individual packets are analyzed, denied content may not be recognized in this partial state and therefore erroneously allowed, or underblocked. To compensate, the router must collect, reassemble, and analyze entire strings of packets (TCP/IP sessions) to understand the entire context of the traffic. However, the more intensive the packet inspection becomes, the greater the burden placed on both the hardware and software within the router. When the inspection process becomes overloaded, the equipment will either fail open, interrupting all traffic including legitimate traffic, or will fail closed allowing all traffic, including undesired traffic, to pass. Either result leads to undesired consequences (Murdoch & Anderson, 2008).

E. DNS TAMPERING

Normal TCP/IP communication relies on IP addresses. However, most users and applications do not initiate communication on the basis of an IP address, rather they utilize URLs and domain names. Domain names are simply human readable and understandable references for Internet resources. Normal TCP/IP communication translates, or resolves, domain names to IP addresses utilizing DNS servers. Resolution requests, or queries, are sent to a client's

predetermined DNS server. That server attempts to answer the request from known information. The action the server takes in the event the server is not immediately able to provide an answer, depends on the configuration of the server, including the possibility to either refer the requestor to another server, or have the requestor wait while the server queries additional servers (Mockapetris, 1987a; Mockapetris, 1987b).

DNS Tampering involves modifying the response with an erroneous answer (Murdoch & Anderson, 2008). Without a valid response to query, the client is unable to proceed with requesting the Internet resource as illustrated in Figure 3. Since it is the name resolution process, rather than the actual TCP/IP traffic, which is interrupted, multiple methods exist for easily circumventing the process. If the user knows the actual IP address of the disallowed resource, the IP address can be utilized for accessing the resource, bypassing the DNS process and negating this filtering technique. Additionally, if alternative DNS servers, rather than our manipulated DNS server, are queried, the correct response may be provided also negating the filtering technique. Since only the blacklisted domain name is utilized for blocking, DNS Tampering is not subject to overblocking of multiple Internet resources when multiple Internet resources share a single IP (Faris & Villeneuve, 2008).

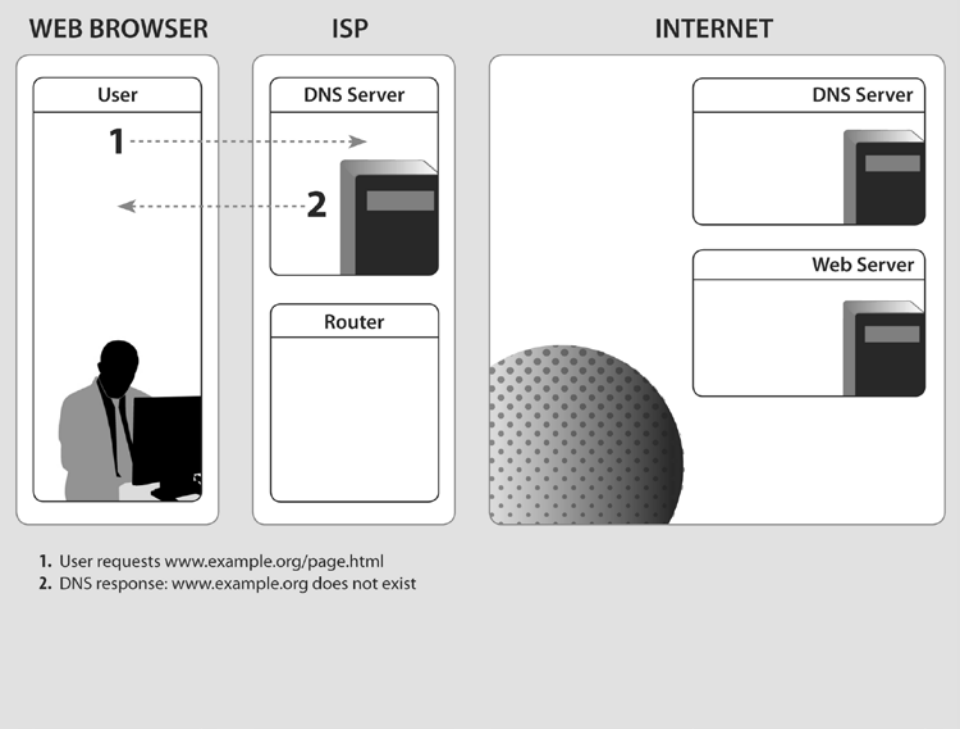

Figure 3 DNS Tampering (After Murdoch & Anderson, 2008)

F. HTTP PROXY FILTERING

Proxy servers are implemented between users and the Internet as a means of limiting user's direct access to the Internet (Murdoch & Anderson, 2008). Instead of directly accessing the Internet, the user submits their request to the proxy server. The proxy server, in turn, accesses the Internet and submits the user's request. The response is provided to and processed by the proxy server. The proxy server then returns the response to the requesting user. Depending on the configuration of the proxy server, the user may or may not realize a proxy server, rather than the Internet, is actually fulfilling their requests. This process is illustrated in Figure 4.

Proxy servers offer a variety of benefits. If multiple users request the same resource from the Internet through the same proxy server, the proxy server need only make a single request to the Internet. In this scenario, the proxy server may cache responses for future reuse. Subsequent client requests could

receive quicker responses while decreasing demands on connections past the proxy server to the Internet (Luotonen & Altis, 1994).

In addition to providing various performance improvements, proxy servers may also be utilized for content filtering. Since all requests and responses pass through the proxy server, the proxy server could be configured to deny requests or responses based on any criteria. In this manner, the proxy server can utilize combinations of TCP/IP Header Filtering and TCP/IP Content Filtering. Since both the entire request and entire response are processed by the proxy server, the server is able to analyze and make determinations based on the full TCP/IP session. This system prevents the server from erroneously allowing blacklisted content based on an analysis of a partial TCP/IP session as is possible in simple TCP/IP Content Filtering. Additionally, since the entire TCP/IP session is available to be analyzed, specific responses containing certain content may be blocked, contrasted with TCP/IP Header Filtering and DNS Tampering where the entire resource would be blocked. Ultimately, proxy servers allow for much finer granularity in blocking over simple TCP/IP Header Filtering, TCP/IP Content Filtering, or DNS Tampering (Ding, Chi, Deng, & Dong, 1999).

While proxy servers may be able to provide superior content filtering through merging of multiple combinations of TCP/IP filtering, they also require significant resources which may not be available for immediate use by an HFN during HA/DR. A proxy server would require either specialized hardware or a dedicated server. Additionally, frequently a proxy server requires specific configuration of client settings to operate properly resulting in additional effort by the user or support personnel.

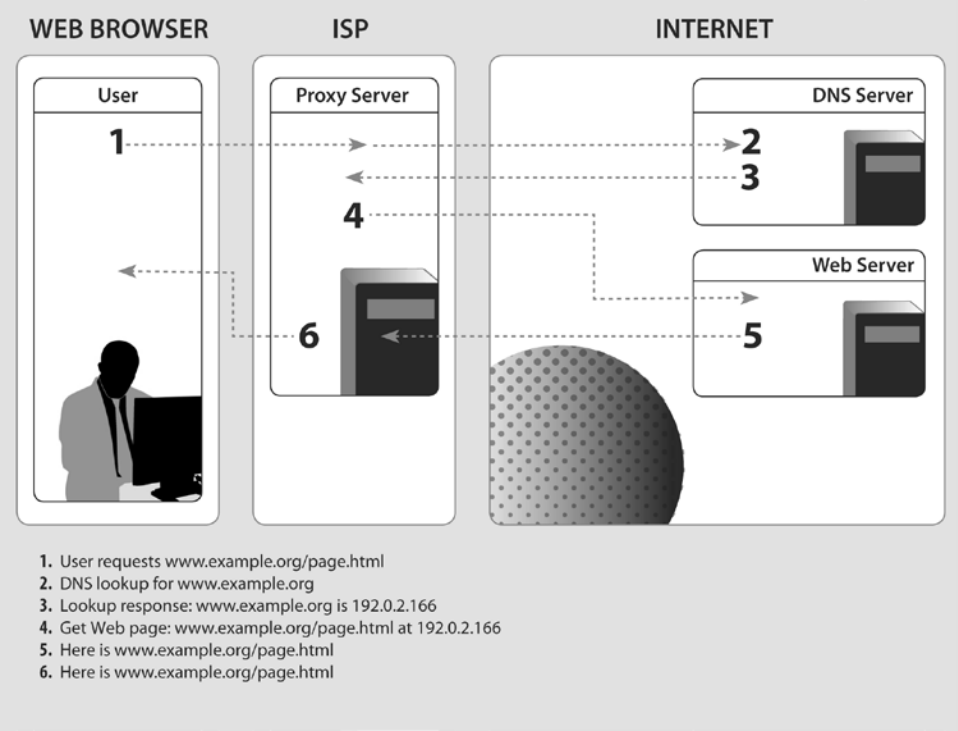

Figure 4 Web Browsing with Proxy Server (After Murdoch & Anderson, 2008)

G. METHODOLOGY OF SELECTION OF CONTENT FILTERING METHOD

Each method of content filtering provides individual benefits as well as being subject to specific weaknesses. Additionally, nearly all content filtering is able to be bypassed if the use of encrypted tunnels, Virtual Private Networks (VPN), is permitted since this traffic would bypass the filters by encrypting the traffic to an outside connection. The ultimate decision for which method of content filtering should be implemented must be based on a variety of factors including control of the network and availability of resources (including equipment, energy, and talent), while balanced with the acceptable risks of overblocking and underblocking. The four methods mentioned were evaluated for application within an HFN and summarized in Figure 5.

TCP/IP Header Filtering blocks content based on addressing information (source or destination). It risks overblocking multiple different resources sharing a single IP address while underblocking resources as addresses change. This

method does not require specific reconfiguration of the workstation and may be able to utilize existing routers within the HFN. Additionally, TCP/IP Header Filtering is not able to be easily circumvented. Unfortunately, the high risk of overblocking based on IP address makes this method less desirable.

TCP/IP Content Filtering blocks resources based on the content of the traffic. This method is subject to overblocking based on content being analyzed out of content and is subject to underblocking by allowing alternatives to blocked content. While this method does not require workstation reconfiguration, it does require specialized hardware capable of performing the packet inspection. Additionally, this method may be circumvented by utilizing alternative representations of blocked content. Ultimately, the requirement for specialized hardware to be implemented in an HFN may make this method unrealistic.

DNS Tampering blocks resources based on the destination name. By blocking all resources which share a single name, DNS Tampering may be subject to overblocking if multiple resources do share a single name. However, this method is not inherently subject to underblocking and does not require reconfiguration of workstations. DNS Tampering may be able to utilize existing routers in an HFN and offsite DNS Services. However, DNS Tampering may be able to be easily circumvented unless the router is able to intercept and redirect DNS queries.

HTTP Proxy Filtering utilizes specialized hardware and software to implement one or more of the other methods of content filtering. Therefore, HTTP Proxy Filtering is subject to the same limitations and risks of the underlying methods. While this method is not able to be easily circumvented, it usually requires reconfiguration of the workstations. Additionally HTTP Proxy Filtering requires specialized hardware and software to be implemented in an HFN which may prohibit implementation of this method.

Ultimately, DNS Tampering appears to provide content filtering while minimizing the risks associated with overblocking and underblocking. These

benefits are provided without requiring workstation reconfiguration or specialized hardware and software within the HFN. The remainder of this research will focus on DNS Tampering as a viable solution for bandwidth management in resource constrained networks.

	Blocking Method	Overblocking Risk	Underblocking Risk	Requires reconfiguration of workstation	Specialized or Additional Hardware required at HFN	Easily circumventable
TCP/IP Header Filtering	Based on source or destination address	Blocks all resources sharing a single address	May not block resources as addresses change	No	May be able to utilize existing routers	No
TCP/IP Content Filtering	Based on packet contents	May block out of context	May not block synonyms	No	Yes	Based on keyword changes
DNS Tampering	Based on destination name	Blocks all resources sharing a single name	None	No	May be able to utilize existing routers with off-site DNS services	Yes, unless router prohibits alternate DNS servers
HTTP Proxy Filtering	Implements one or more methods	Based on implemented method	Based on implemented method	Usually	Usually requires onsite server	No

Figure 5 Comparison of Content Filtering Methods

THIS PAGE INTENTIONALLY LEFT BLANK

III. DESCRIPTION OF METHODOLOGY AND EXPERIMENTS

Our experiments tested DNS Tampering in reliability and practicality as a method of content filtering. The experiments measured reliability in terms of accurately blocking undesired content. We evaluated practicality by ease of administration. For the purpose of this research, we focused on the update services built into Windows XP and Windows 7 since these two operating systems accounted for the largest user base both shortly after the time of the Haitian earthquake and now (W3Schools, 2012).

Our research questions are:

- How can network traffic for specific applications be filtered utilizing DNS Tampering?
- How is bandwidth affected by reducing this traffic?
- What are the requirements to implement DNS Tampering into an HFN?

A. EXPERIMENTAL SETUP

The experiments were conducted in a virtual machine environment running VMware Workstation 7.1. The operating systems tested were Microsoft Windows XP and Microsoft Windows 7. Figure 6 depicts our logical network diagram. The guest operating systems were connected to the inside interface of a Linksys WRT-54G broadband router running Tomato 1.28 firmware. Packet capture was performed on the outside interface of the router utilizing a separate computer running Wireshark 1.6.4. The outside, rather than inside, interface was used in order to limit the amount of traffic available for capture since the router will prevent traffic local internal traffic from passing to the outside interface. The outside interface, the packet capture computer, and the Internet uplink were all connected together via a network hub rather than a network switch. Network switches operate at Data Link layer of the Open Systems Interconnection (OSI) model allowing them to route traffic based on MAC address (Kurose & Ross, 2009). While switching technology is generally desired in most networking

operations, it would have routed traffic from the router's outside interface directly to the Internet uplink, bypassing our packet computer. Network hubs are considered to operate at the Physical Layer of the OSI model and retransmit incoming traffic to all ports (Kurose & Ross, 2009). By connecting the outside interface, packet capture computer, and Internet uplink together via a hub, all traffic destined for either the outside interface or Internet uplink was transmitted to all ports including our packet capture computer.

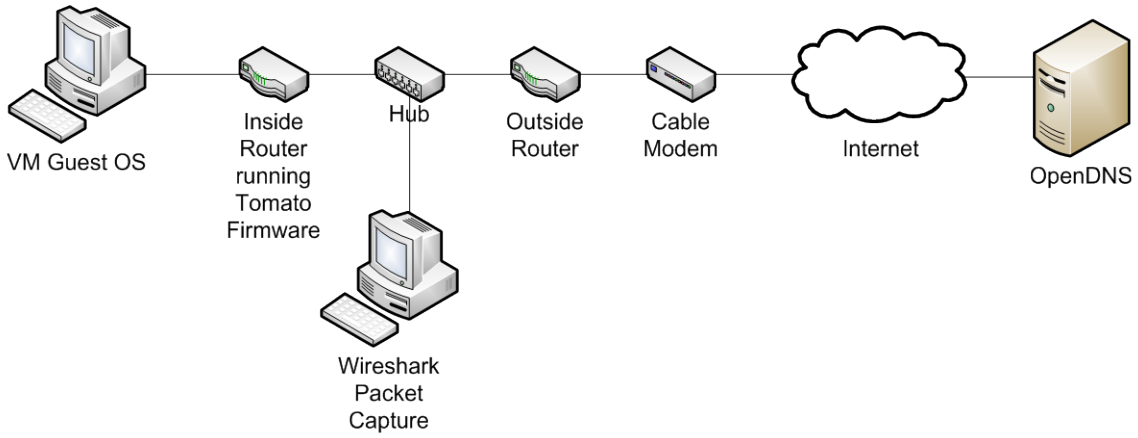

Figure 6 Logical Network Diagram

Utilizing virtual machines for testing allowed for multiple iterations of experiments to be tested easily. Snapshots, or system states, of each virtual machine may be saved allowing easy access to different points in time. Each system could be rolled back to a previous configuration for further testing and evaluation without requiring external backup and restore or reinstallation of systems. This expedited the testing process and allowed multiple rapid tests and evaluations while minimizing required effort and time.

Tomato firmware, an alternative to the well-known DD-WRT firmware, is an open source firmware installable on a variety of commercial routers. Tomato extends the feature set and functionality of the stock firmware contained in most consumer class routers (Zarate, 2011). While both DD-WRT and Tomato were evaluated, it was determined that DD-WRT required the router to be rebooted

each time a configuration change was made. This made frequent and rapid changes to the router configuration a cumbersome and lengthy process. Tomato allowed changes to be committed without requiring a reboot of the router. Instead, only router restarted the necessary processes within the firmware saving considerable time. Additionally, Tomato provided better bandwidth monitoring capabilities allowing real-time (Figure 7) and historical (Figure 8) data usage for evaluation in the experiments.

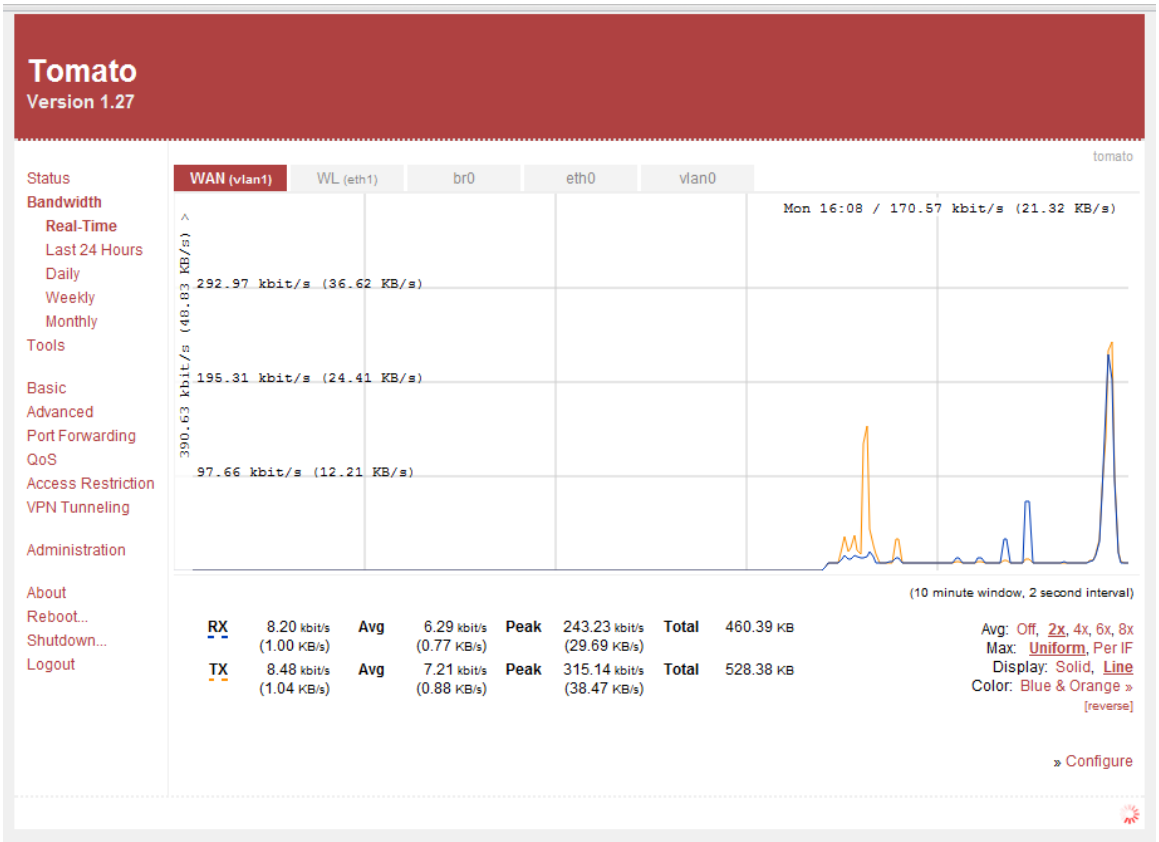

Figure 7 Tomato Real-Time Bandwidth Sample

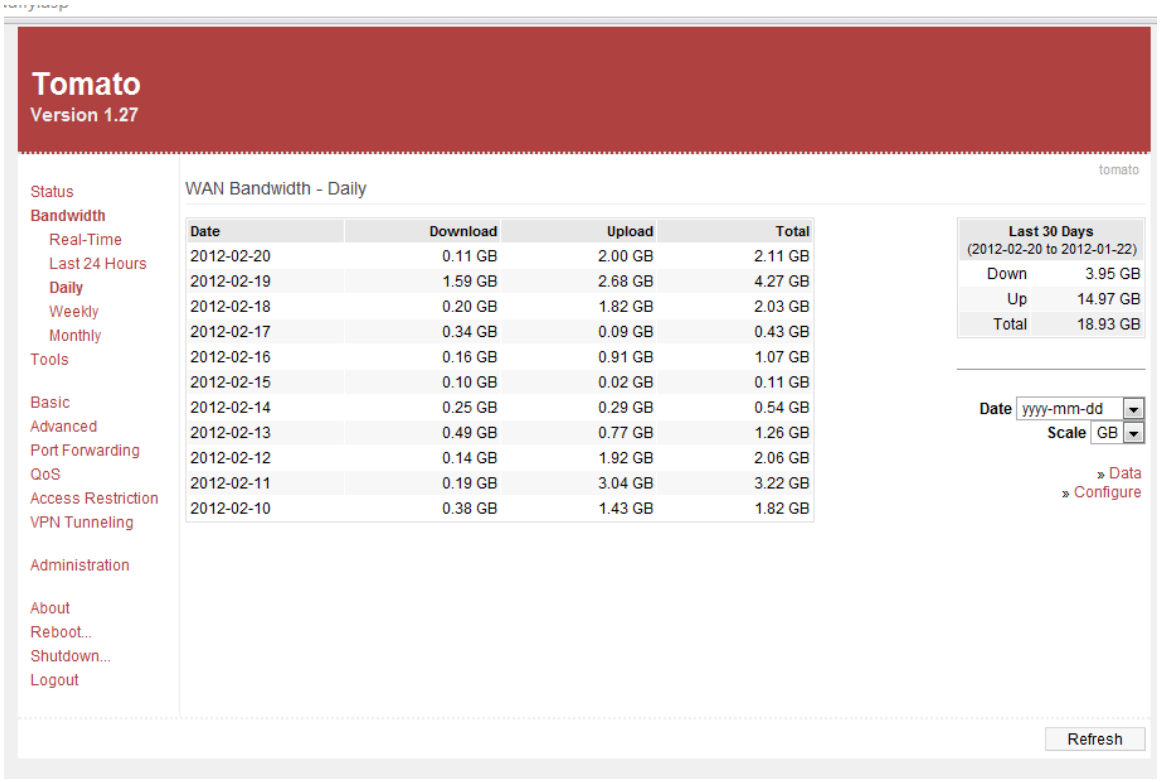

Figure 8 Tomato Historical Bandwidth Sample

Tomato firmware was configured to utilize a single OpenDNS server, 208.67.222.222, for DNS queries as shown in Figure 9. OpenDNS is a commercially available DNS service providing the ability to manage and alter DNS information for the end user. The company suggests the ability to "increase the speed of navigating websites and prevent unintended access to phishing and malware sites as well as to any Web content that you configure to be restricted" (OpenDNS, 2011). Although OpenDNS does provide IP addresses for two DNS servers, and best practices would implement both servers, this could lead to multiple DNS queries for each DNS request. During normal network operations, multiple DNS queries would not be a significant issue. However, for the purpose of this research, the elimination of multiple repetitive queries was desirable.

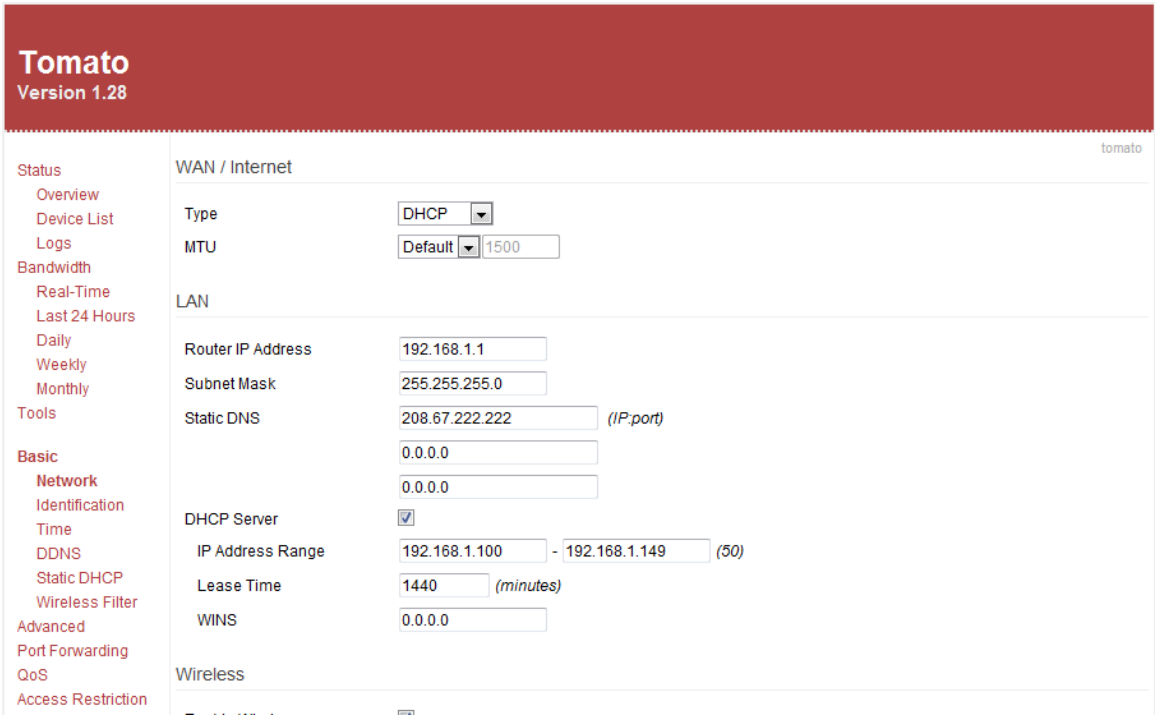

Figure 9 Tomato DNS Servers

DNS queries are normally conducted on User Datagram Protocol (UDP) port 53 (Mockapetris, 1987a; Mockapetris, 1987b). Normally the router is configured to query specific DNS servers, and through the Dynamic Host Configuration Protocol (DHCP) the router specifies clients query the router for DNS requests. However, alternate DNS settings may be manually specified in the client configuration. When this occurs, the client will utilize the manually specified settings rather than those provided by the router (Alexander & Droms, 1997). This configuration may allow the client to utilize DNS services undesired by the administrator. To prevent queries being passed to unauthorized external DNS servers Tomato offers the option, Intercept DNS port (UDP 53), to intercept DNS queries as displayed in Figure 10 (Zarate, 2011). This setting and functionality was verified through a series of tests.

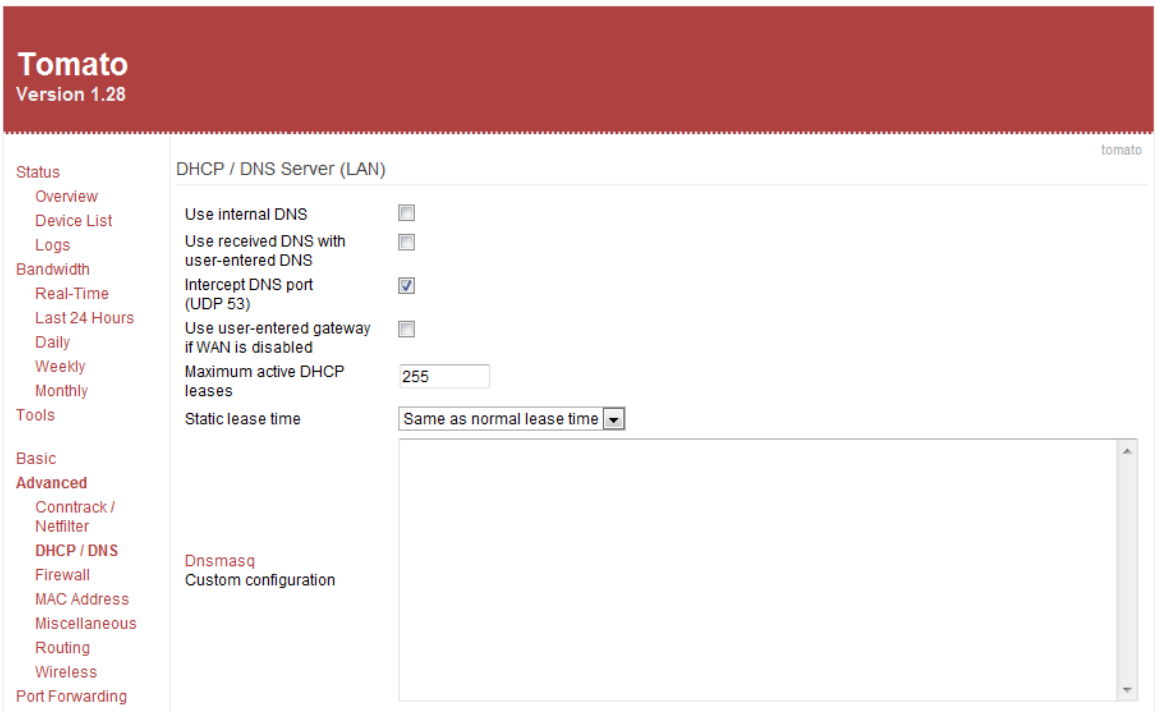

Figure 10 Tomato DNS Server Options

Initially, we verified the option to Intercept DNS port (UDP53) was set to disabled. The command line tool NSLOOKUP was used to query google.com as shown in Figure 11. Wireshark packet capture verified the query was passed to our specified OpenDNS server as shown Appendix A, Annex 1. A series of 11 results, all in the 74.125.224.x address space, were returned. We also verified we could browse to google.com via a web browser.

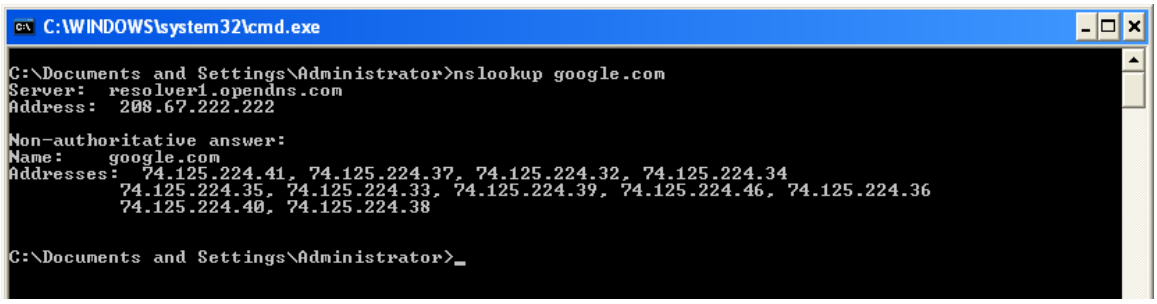

Figure 11 Normal NSLOOKUP without Tomato Intercepting DNS Queries

We then listed google.com as a blocked domain in OpenDNS as displayed in Figure 12 and repeated the NSLOOKUP query. This instance returned a single IP address of 67.215.65.131 as shown in Figure 13 and Appendix A, Annex 2. When we attempted to browse to google.com via a web browser, we received a notification page indicating www.google.com was indeed blocked as shown in Figure 14.

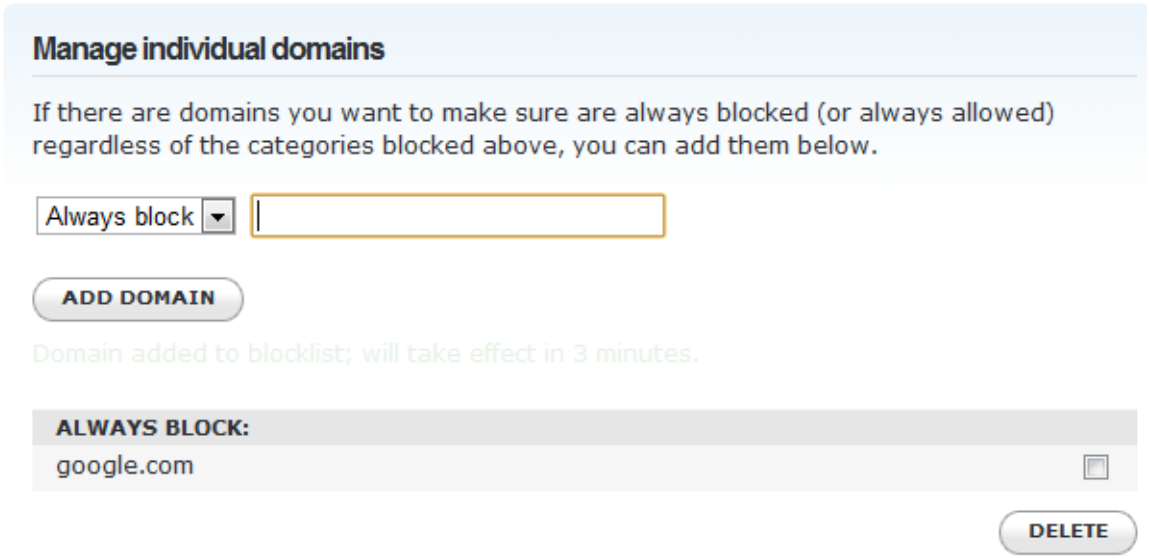

Figure 12 OpenDNS Blocking Google.com

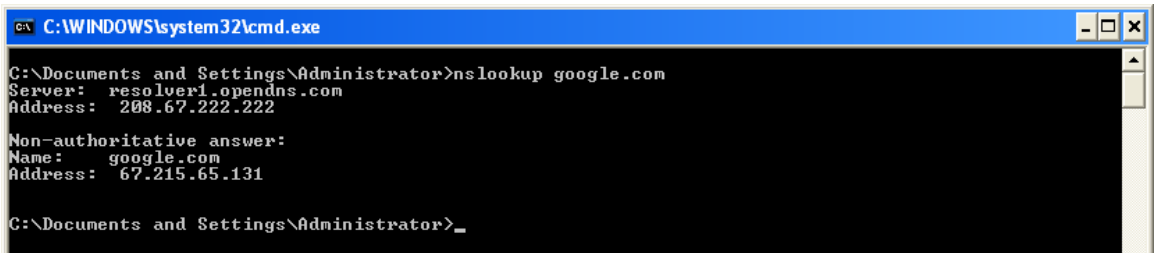

Figure 13 NSLOOKUP of Blocked Domain without Tomato Intercepting DNS Queries

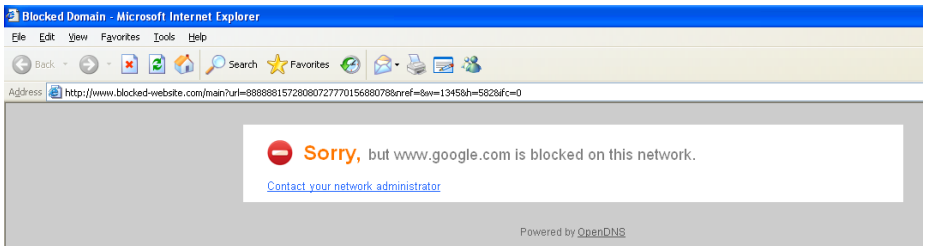

Figure 14 Web Browsing to Blocked Domain google.com

We now attempted to bypass the internally specified OpenDNS server by directing an NSLOOKUP query to an alternative public DNS server as shown in Figure 15. Once again, google.com resolved to the original 11 separate IP addresses indicating that our query was indeed redirected from our specified OpenDNS server to an alternate server. Wireshark confirmed that our DNS request passed to our specified alternative server rather than the default OpenDNS server as shown in Appendix A, Annex 3.

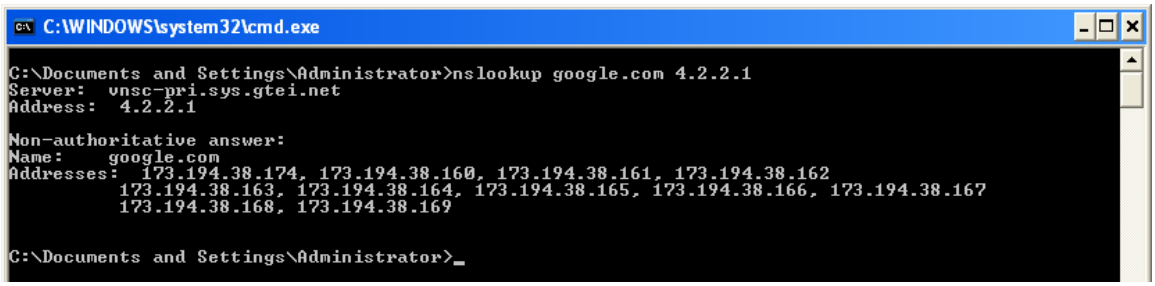

Figure 15 NSLOOKUP of Blocked Domain to Alternative DNS Server without Tomato Intercepting DNS Queries

We enabled the option within Tomato to Intercept DNS port (UDP53) as displayed in Figure 10 forcing all DNS traffic to our specified OpenDNS server. We repeated the query of google.com while specifying our alternative DNS server. However, this time, even when specifying an alternative DNS server, our NSLOOKUP returned the single IP address of 67.215.65.131 as displayed in Figure 16. Further, Wireshark indicated that our DNS query was indeed passed to and returned from the OpenDNS server rather than the specified alternative

DNS server as demonstrated in Appendix A, Annex 4 Packet Capture of DNS Query of Blocked Domain to Alternative DNS Server With Tomato Intercepting DNS Queries.

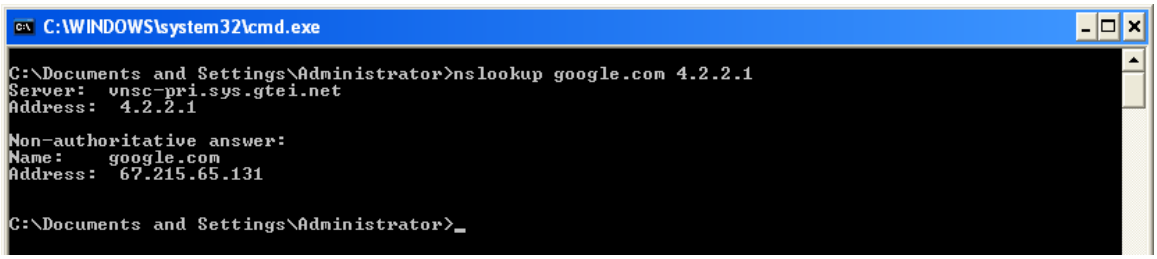

Figure 16 NSLOOKUP of Blocked Domain to Alternative DNS Server with Tomato Intercepting DNS Queries

B. EXPERIMENTS

The first experiment evaluated the native update services of both Windows XP and Windows 7 in an unrestricted OpenDNS environment utilizing a commercially available, consumer class Internet connection. This experiment gathered baseline information to be utilized in further experiments.

The second experiment utilized the results from experiment one to test effectiveness of DNS tampering utilizing OpenDNS combined with the same consumer class Internet connection. We measured significant reductions in network utilization as our *blacklisted* traffic was eliminated.

The third experiment measured traffic utilizing OpenDNS with a satellite Internet provider similar to what would be available during a HA/DR. Traffic was measured both with and without DNS Tampering. The goal was to determine the effectiveness of this technique for limiting traffic utilizing equipment available for real world scenarios.

1. Experiment One Setup

The first experiment utilized initial, or clean, installations of Windows XP and Windows 7. Both operating systems were installed as guest operating systems on VMware Workstation 7.1. This configuration allowed easy roll back

to various reference points in time through the use of snapshots. We configured Tomato to utilize OpenDNS for DNS resolution.

We installed each operating system and configured Microsoft's Automatic Updates. Wireshark was used to record and analyze the Internet traffic on the external interface of the router. The experiments were conducted over approximately a one week period utilizing a variety of configurations. We evaluated the recordings from Wireshark and determined which DNS records were utilized for each operating system's updates. Specific DNS records were identified as being associated with these processes. Bandwidth requirements for the various updates were also recorded to be used in further comparisons.

2. Experiment Two Setup

For Experiment Two we utilized the results from Experiment One to limit access to specific resources on the Internet. We intended to show that access to the Internet could be limited for specific applications through the use of DNS Tampering. We configured Tomato to utilize OpenDNS for DNS resolution. Utilizing the DNS records identified in Experiment One, we implemented specific domain blocking through OpenDNS's web interface. We allowed our operating systems and applications to attempt various automatic updates and monitored Internet usage. We continued to test other forms of Internet access to verify otherwise normal usage.

3. Experiment Three Setup

For Experiment Three we repeated Experiments One and Two utilizing a commercially available BGAN for Internet access. With the exception of changing the connection to the Internet, the balance of the equipment and tests remained the same. We first configured Tomato to utilize OpenDNS for DNS resolution and ensured OpenDNS was not configured to block resources. We performed various updates to ensure the systems were operating normally as we did in Experiment One. We then configured OpenDNS to block access to specified resources as in Experiment Two and repeated the updates.

IV. DISCUSSION OF RESULTS

The first challenge discovered during initial experimentation was the overwhelming amount of information returned from Wireshark. Being able to differentiate between traffic relevant to the research and what traffic was simply background noise proved difficult at times. Isolating the packet capture workstation between two routers reduced all extraneous network traffic. Utilizing snapshots through VMware permitted repeated, controlled experiments and allowed the refinement of the data collection process. Ultimately, Wireshark's ability to specifically filter DNS traffic reduced the amount of data to review (Wireshark, 2008).

An additional challenge was Window's ability to cache DNS information. As Windows performs DNS queries, it caches the results for future use. This improves response time by reducing the number of requests to the network (Microsoft, 2007). However, for the purpose of testing, it meant that a single DNS request could be cached and used multiple times in the future by multiple different requesting applications. Since a DNS query may not be initiated during each download after an update was selected, it was unclear if the update process was relying on DNS caching of some sort or if that particular update was utilizing communications which did not rely on DNS. To ensure accurate analysis of the different applications, Client-Side DNS Caching was disabled by stopping the dnsclient service (Microsoft, 2007). Although the article specifically referenced Windows XP, it was equally applicable to our Windows 7 environment. Additionally, several minutes (usually between 5 and 10) were allowed to pass between selecting an update and actually initiating download in an attempt to force the expiration of whatever DNS information may be cached in the update application.

Tomato implements dnsmasq as "a lightweight DHCP and caching DNS server" (Kelley, 2011). This enables the router to cache DNS responses in an effort to improve response time and reduce demands on upstream DNS

resources. As with client-side DNS caching, this made reliable analysis difficult. Utilizing instructions from the manpage, dnsmasq caching was disabled by setting the option for cache-size to zero, forcing the router to submit new queries for each client query received (Kelley, 2011).

A. EXPERIMENT ONE

The data collected from Experiment One showed Windows XP and Windows 7 use specific DNS records during both manual and automatic updates.

1. Windows XP Manual Update

During the initiation of a manual update process on Windows XP, four separate DNS queries were captured with Wireshark:

- windowsupdate.microsoft.com
- www.update.mircosoft.com
- download.windowsupdate.com
- c.microsoft.com

It was evident that the first three queries all related to the update process. However, the purpose of the fourth DNS query, c.microsoft.com, was not immediately evident. Further evaluation of the Transmission Control Protocol (TCP) stream captured with Wireshark determined c.microsoft.com was utilized for the purpose of setting a browser cookie during the manual update process but was not directly related to the update process. All of these queries were performed during the initial launching of the manual update process during which the web browser determined what updates were available for installation, but are not already installed.

We selected a single 485 kilobyte (KB) update and monitored our bandwidth usage utilizing Tomato. As seen in Figure 17, the entire update process, including selecting and downloading the update, consumed a total of 804.80 KB of bandwidth (610.27 KB received and 194.53 KB transmitted). The results from Wireshark as displayed in Appendix B, Annex 1.

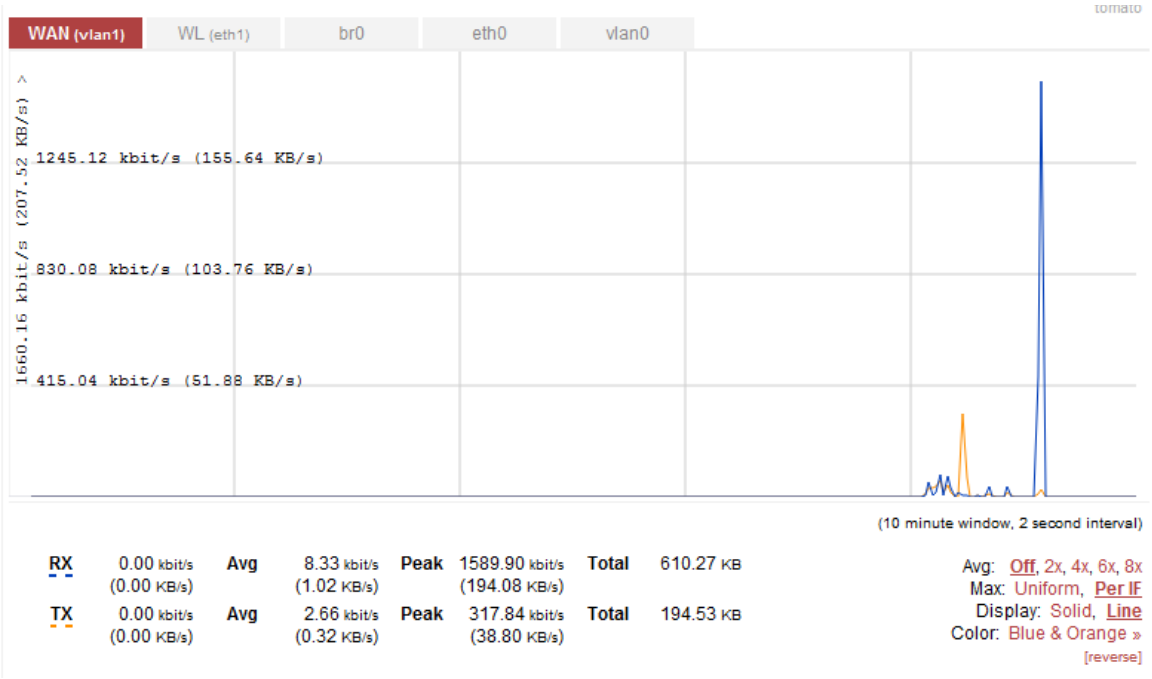

Figure 17 Normal Windows XP Manual Update

2. Windows XP Automatic Update

When configured for automatic updates, Windows XP makes three separate DNS queries identical to the first three queries of the manual update process:

- windowsupdate.microsoft.com
- www.update.mircosoft.com
- download.windowsupdate.com

It was not unexpected that the automatic update application did not rely on browser cookies during the update process. Rather, the application would handle the history of updates installed and updates available. During the actual downloading and installation of updates through the automatic update process, au.download.windowsupdate.com was utilized for obtaining the download. This difference from the manual update process was unexpected.

We allowed the automatic update process to download a single update of 489 KB which consumed 700.79 KB of bandwidth (557.61 KB received and

143.18 KB transmitted) as shown in Figure 18. The results from the Wireshark packet capture are displayed in Appendix B Annex 2.

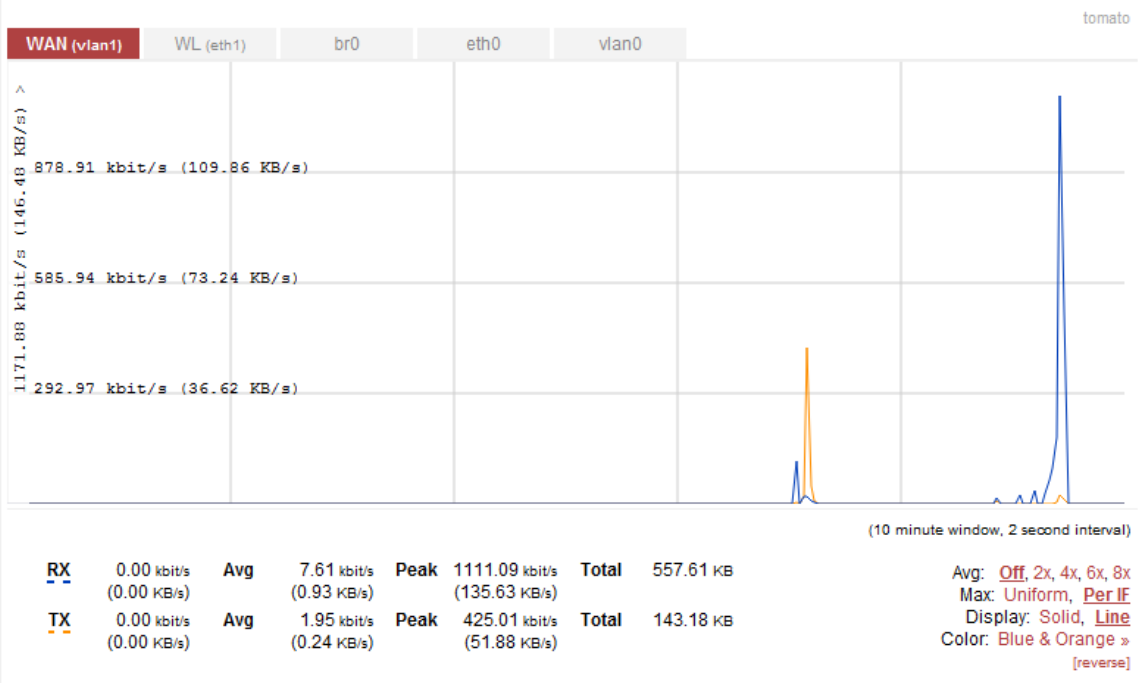

Figure 18 Normal Windows XP Automatic Update

3. Windows 7 Manual Update

Windows 7 updates were conducted with similar results. The notable exception is that while manual updates for Windows XP are conducted through the web browser, manual updates for Windows 7 are completed through an applet in the control panel. The manual update produced three DNS queries:

- download.windowsupdate.com
- www.update.microsoft.com
- www.download.windowsupdate.com

While slightly different than the Windows XP manual updates, the results were very similar. After the initial DNS queries, the update process formed a list of updates available for download. The actual downloading of updates was identical to the Windows XP process in utilizing a DNS query for download.windowsupdate.com.

We performed a manual update selecting a single 499 KB file. The update process utilized 3,237.50 KB of bandwidth (2,666.70 KB received and 570.80 KB transmitted) as shown in Figure 19. Appendix B, Annex 3 displays the results of the Wireshark packet capture.

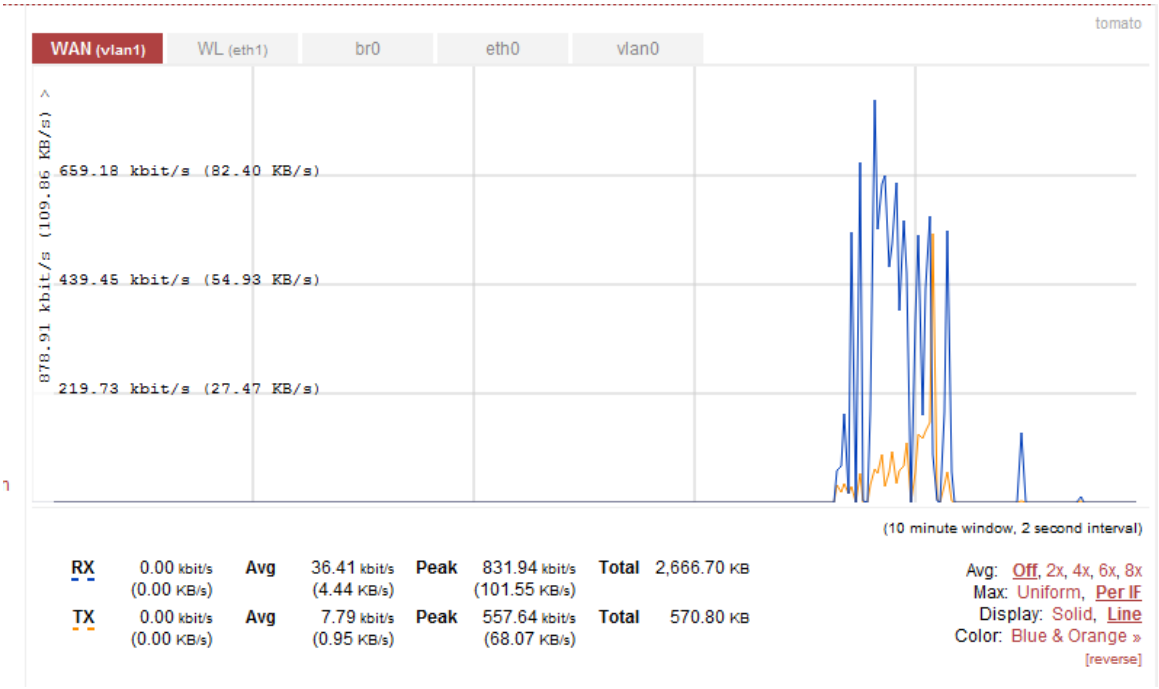

Figure 19 Normal Windows 7 Manual Update

4. Windows 7 Automatic Update

Automatic updates for Windows 7 utilized two previously documented DNS queries to assemble a list of available updates:

- download.windowsupdate.com
- www.update.microsoft.com

We selected a single 499 KB update utilizing the automatic update process. Figure 20 displays a total of 3,197.31 KB (2,654.08 KB received and 543.23 KB transmitted) of bandwidth was utilized during the update process. The Wireshark packet capture results are displayed in Appendix B, Annex 4.

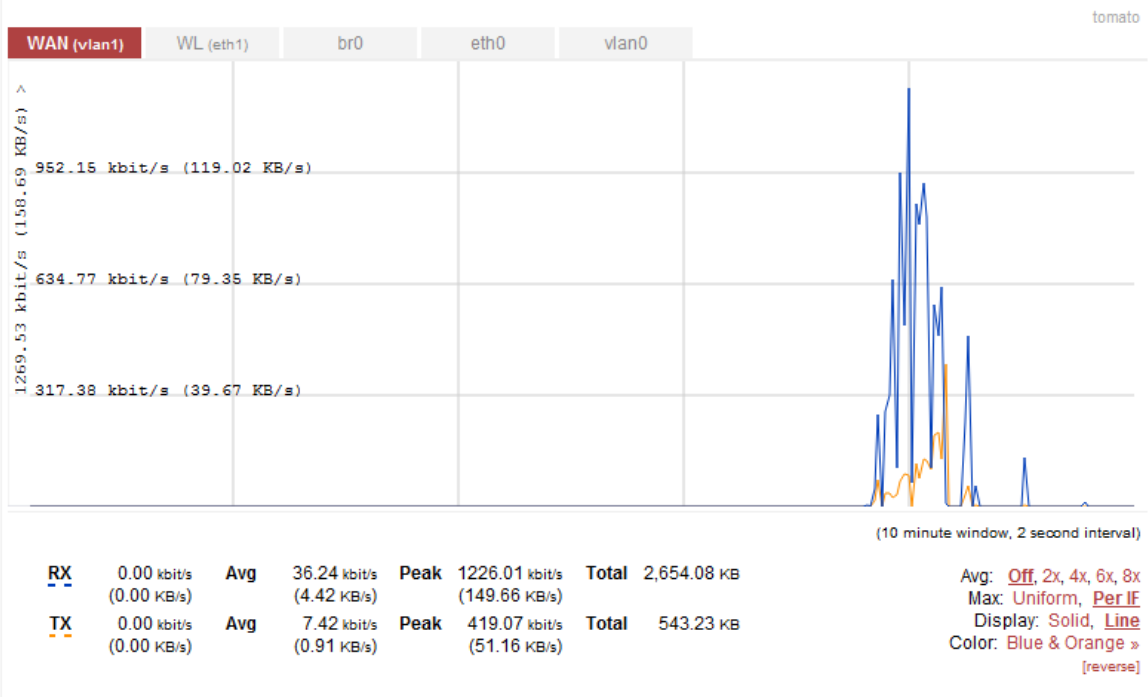

Figure 20 Normal Windows 7 Automatic Update

5. Conclusion

Ultimately, all Windows XP and Windows 7 updates queried some combination of six distinct DNS records:

- c.microsoft.com
- www.update.microsoft.com
- windowsupdate.microsoft.com
- download.windowsupdate.com
- au.download.windowsupdate.com
- www.download.windowsupdate.com

The record c.microsoft.com was used strictly by Microsoft for the purpose of setting and controlling cookies and was not specifically involved in the software updating process. The remaining five records all belonged to three parent domains:

- update.microsoft.com
- windowsupdate.com
- windowsupdate.microsoft.com

B. EXPERIMENT TWO

OpenDNS blocks all subdomains rather than strictly a parent domain. Instead of listing all five domains utilized for updating identified in Experiment One, only the two parent domains were required to be entered in OpenDNS for blocking as shown in Figure 21. While this simplifies the configuration, it does risk overblocking in the case when a subdomain which should be accessible is not. We verified the domains were blocked by performing a command line query using NSLOOKUP for all five domains against our default OpenDNS server as shown in Figure 22. The confirmed the names each resolved to 67.215.65.131, the IP address we previously determined was provided by OpenDNS for blocked domains. Additionally, when the domains were queried against an alternative DNS server, the request was intercepted and redirected to our default OpenDNS server as shown in Figure 23. This ensured that even if an application attempted to resolve names utilizing DNS with an alternative server, the requests would still be processed by our designated server.

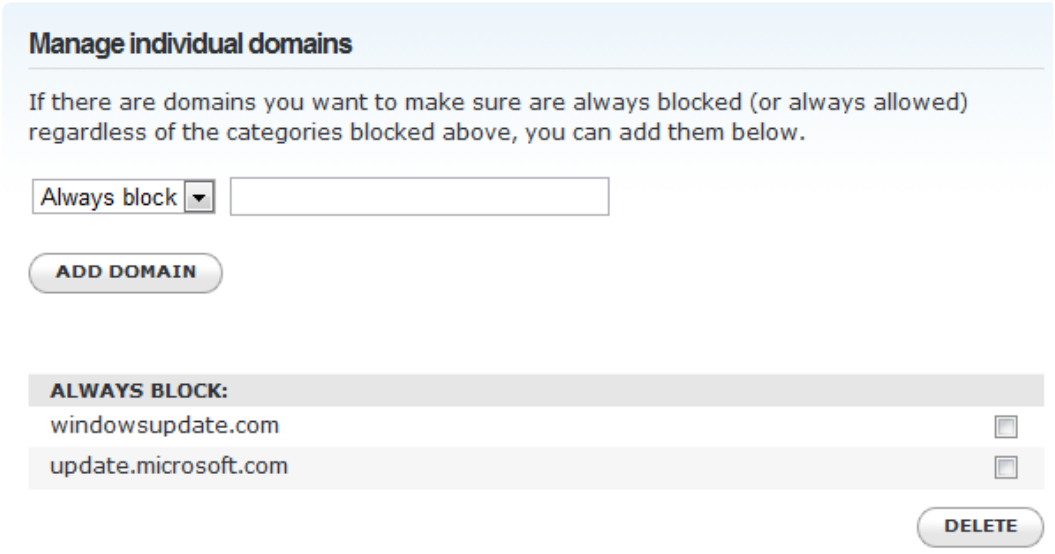

Figure 21 OpenDNS Blocking windowsupdate.com and update.microsoft.com

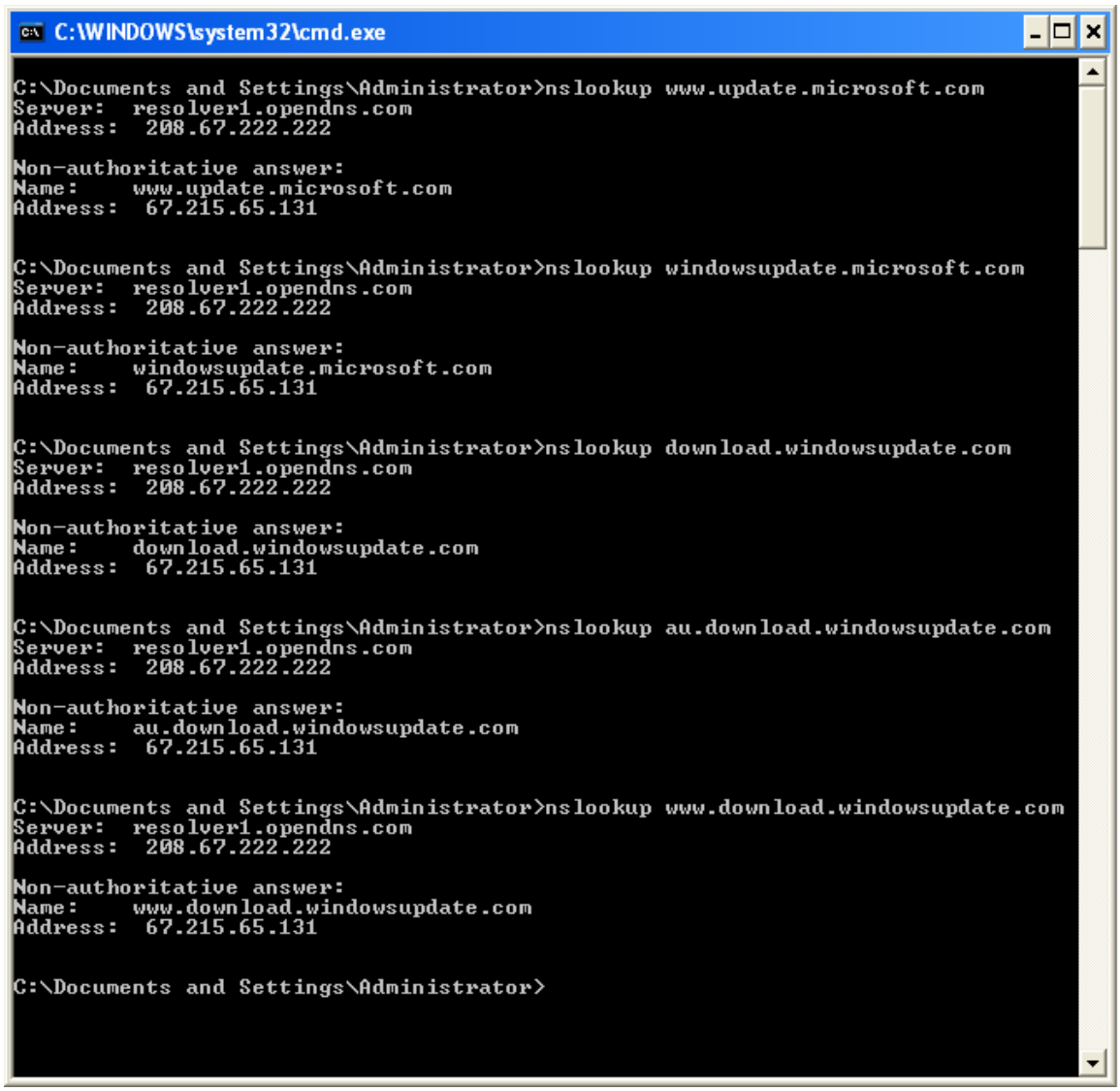

Figure 22 NSLOOKUP Verifying Blocked Domains

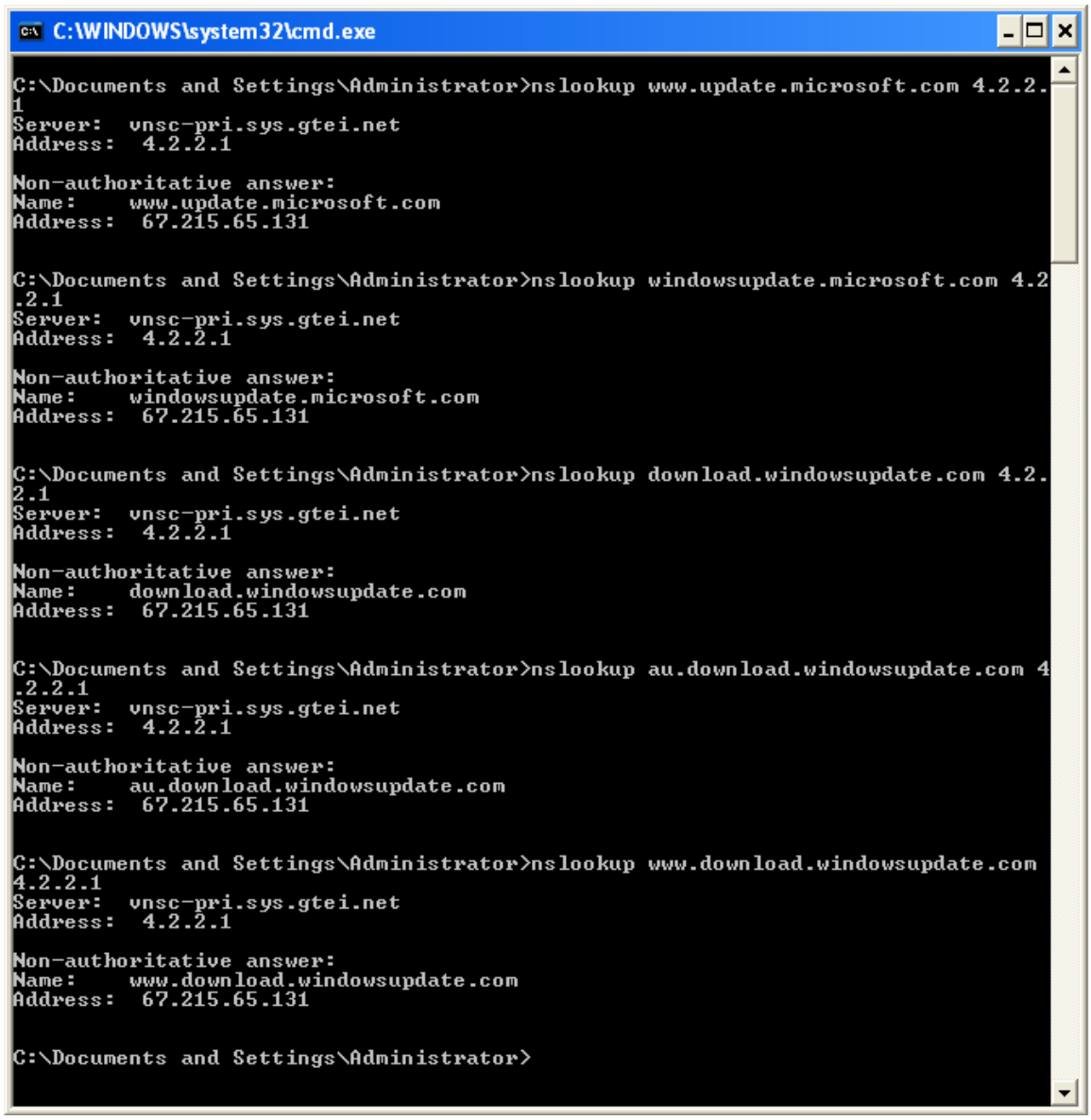

Figure 23 NSLOOKUP Verifying Intercepted DNS Queries

1. Windows XP Manual Update

Initiating a manual update of Windows XP through both the Start Menu and directly through a web browser both resulted in a message from OpenDNS stating the resource was blocked as shown in Figure 24. Packet captures from Wireshark show the DNS queries for the updates resolving to 67.215.65.131, an IP address OpenDNS utilizes for redirecting blocked domains, shown in

Appendix C, Annex 1. The total bandwidth requirement was 286.41 KB (215.15 KB received and 71.26 KB transmitted) as shown in Figure 25.

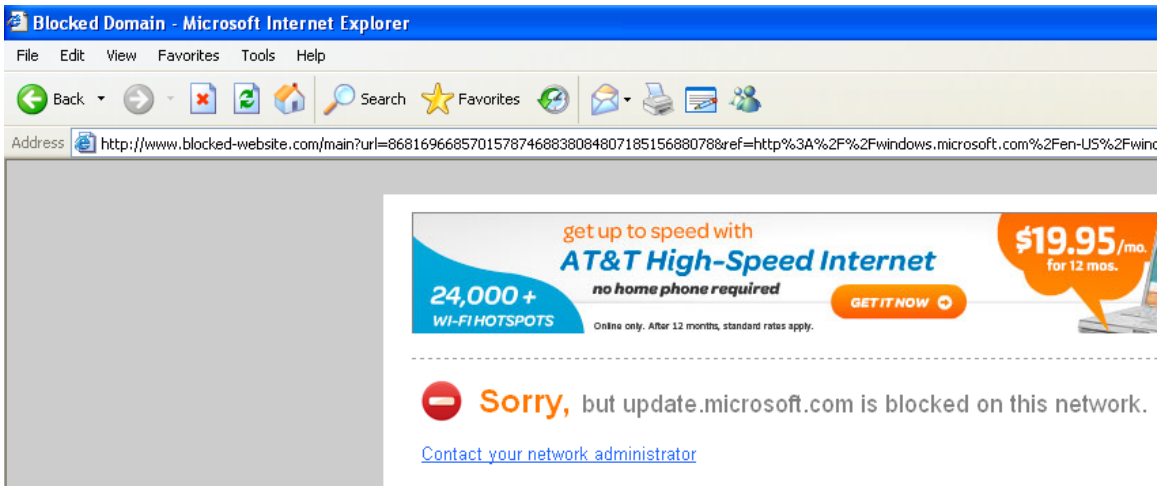

Figure 24 OpenDNS Blocked Message

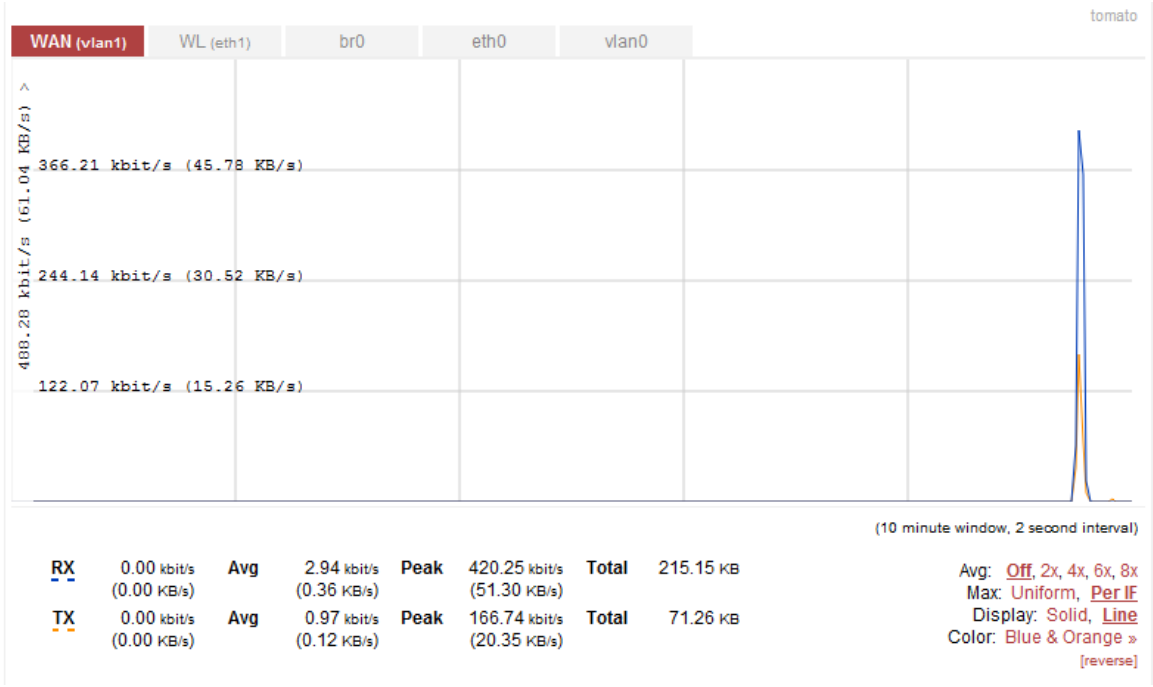

Figure 25 Blocked Windows XP Manual Update

2. Windows XP Automatic Update

Automatic updates in Windows XP did not produce any visible message on the workstation. The workstation provided no indication it was attempting to perform any updates. However, the Wireshark packet capture did display the DNS queries required for Windows updates along with the response from OpenDNS indicating the domains were blocked as displayed in Appendix C, Annex 2. This iterated through a single update attempt indicating that the automatic update will only make two DNS queries per update cycle and will not make repeated failed update attempts. The total bandwidth used was 5.443 KB (2.856 KB received and 2.587 KB transmitted) as shown in Figure 26.

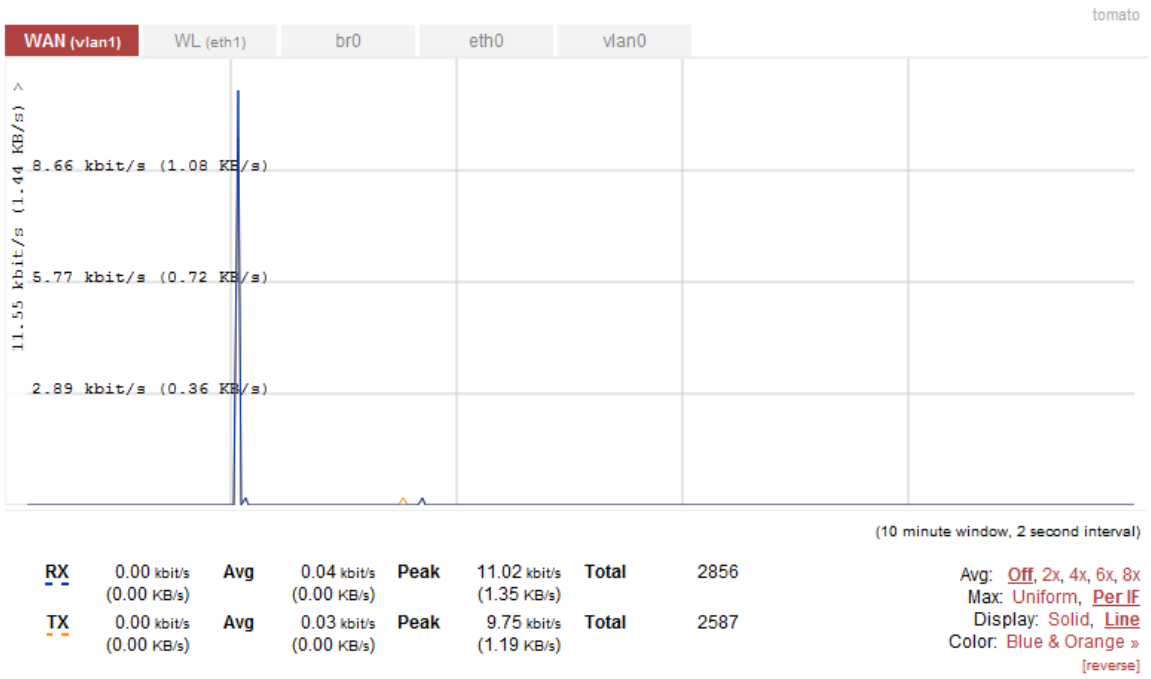

Figure 26 Blocked Windows XP Automatic Update

3. Windows 7 Manual Update

Utilizing the control panel applet in Windows 7 to perform a manual update failed to display a list of updates. Instead, the screen displayed an error code 80244019 along with a link to suggestions on ways to resolve the issue. This message is shown in Figure 27. However, none of the suggested corrections

were able to resolve the error. Wireshark confirmed the update process failed to properly resolve the necessary DNS records and instead returned the redirected records from OpenDNS as displayed in Appendix C, Annex 3. Figure 28 shows a total of 6.655 KB of bandwidth (3.656 KB received and 2.999 KB transmitted) during the update attempt. While the blocking of the updates was successful, the non-descript error could prove misleading and troublesome to users.

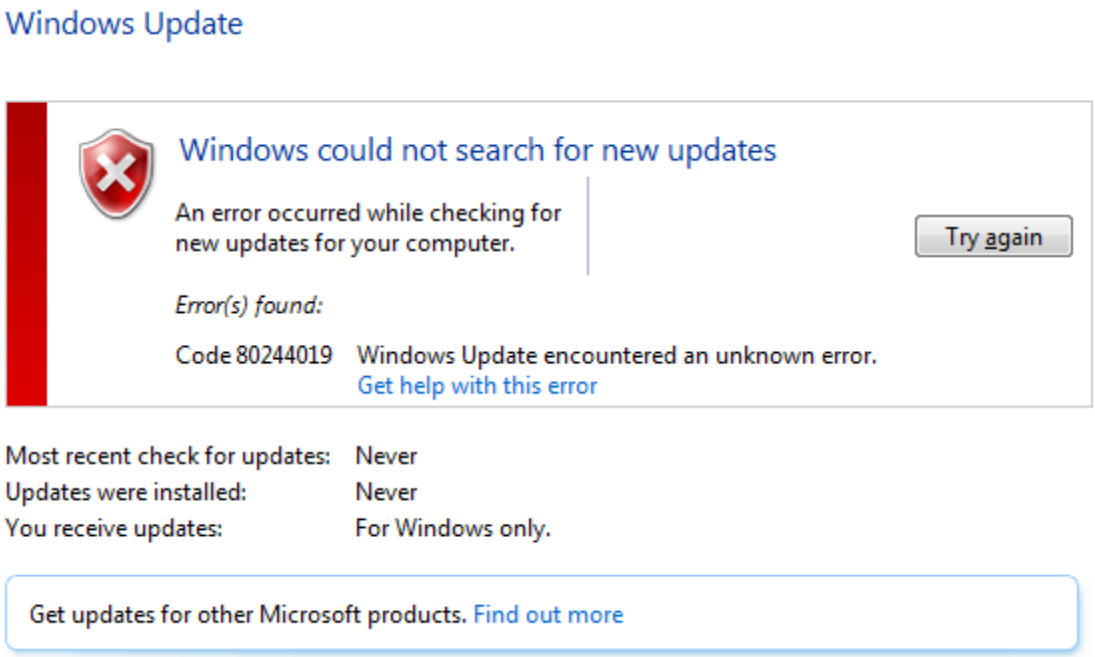

Figure 27 Windows 7 Update Error Message

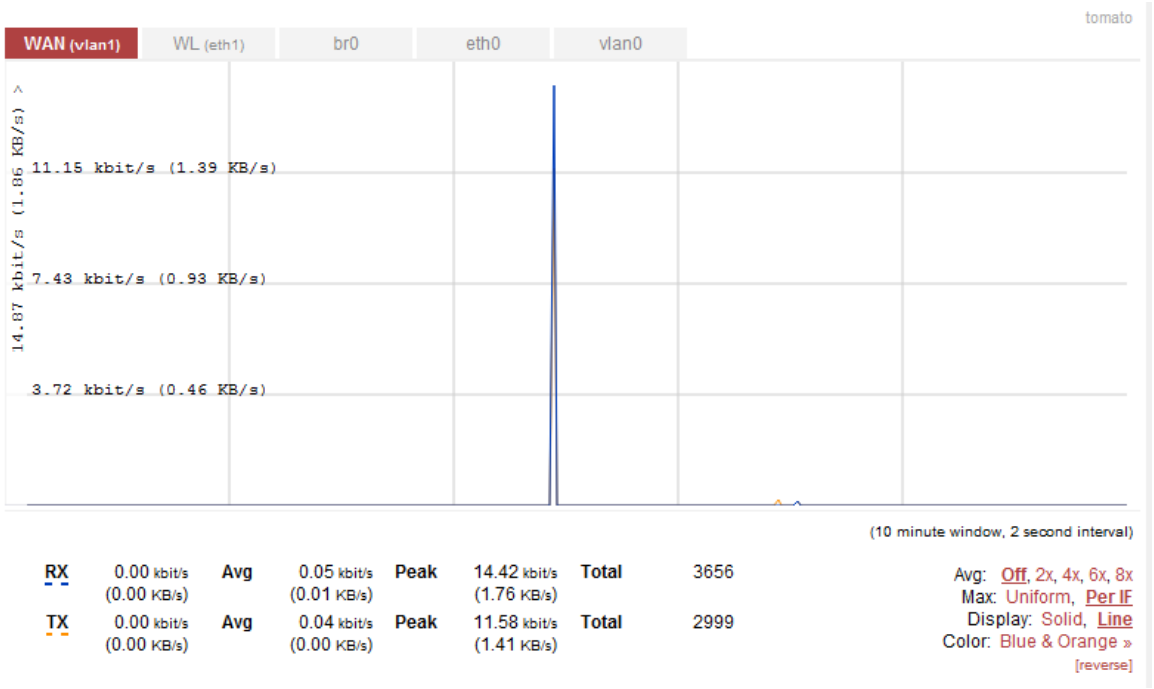

Figure 28 Blocked Windows 7 Manual Update

4. Windows 7 Automatic Update

The Windows 7 automatic update responded in the same manner as the Windows XP automatic update. The workstation provided no indication it was attempting an update. However, the control panel applet did display the same error message as the Windows 7 manual update as shown in Figure 27. Wireshark captured the DNS queries and displayed the redirected DNS results from OpenDNS as shown in Appendix C, Annex 4. Figure 29 displays the total bandwidth utilized was 7.033 KB (3.944 KB received and 3.089 KB transmitted).

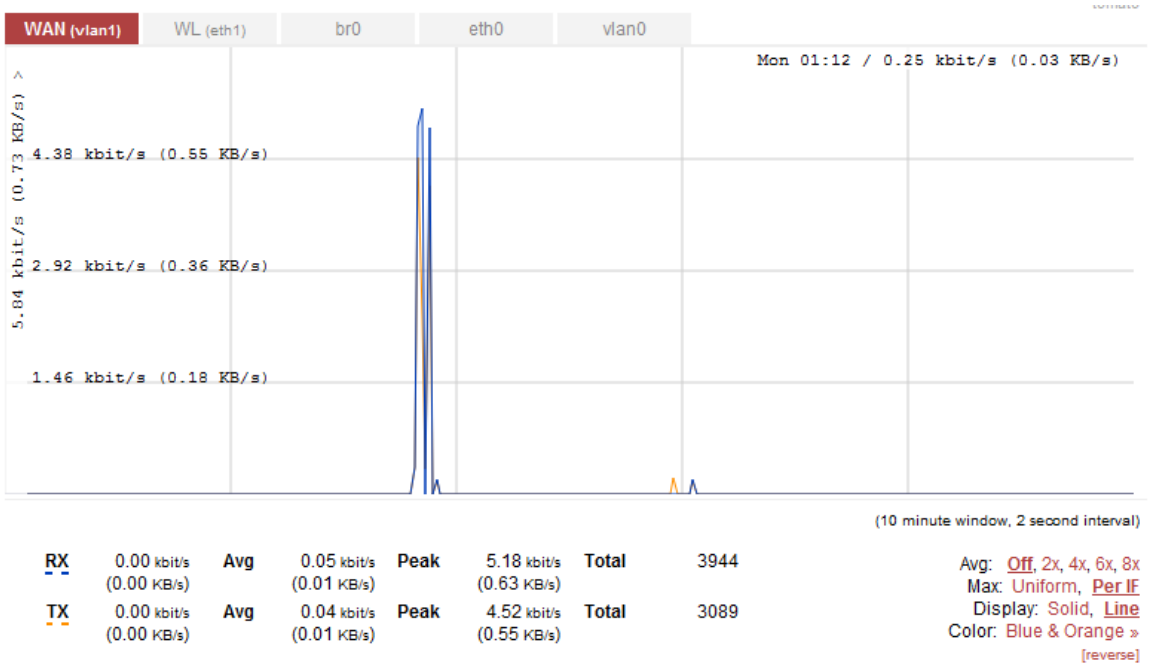

Figure 29 Blocked Windows 7 Automatic Update

5. Conclusion

Utilizing DNS Tampering through domain blocking with OpenDNS prevented both automatic and manual updates on Windows XP and Windows 7. In all cases, the workstations were unable access the list of available updates as well as were unable to access content to download. In the case of Windows XP manual updates, a message was displayed to the user explaining the resources were blocked. In the case of Windows 7 manual updates, an error code was displayed which could alarm users and administrators.

C. EXPERIMENT THREE

Experiment Three evaluated our findings utilizing a commercially available Thrane & Thrane Explorer 700 BGAN. In addition to serving as an Internet access device, the BGAN also acts as traditional consumer grade router providing basic the basic networking services of Network Address Translation (NAT), DHCP, DNS, and Wireless Access Point (WAP). While this all-in-one concept is efficient for deployment, the configuration limitations within the

interface prevent implementing DNS Tampering without additional hardware. Specifically, the web enabled configuration interface did not allow specifying alternative DNS servers for either the workstations or router to utilize. Figure 30 demonstrates the limited configuration options of the Thrane & Thrane Explorer 700 BGAN. To utilize DNS Tampering with the Thrane & Thrane BGAN, we replicated our configuration from Experiments One and Two and utilized Tomato to specify and control our DNS settings.

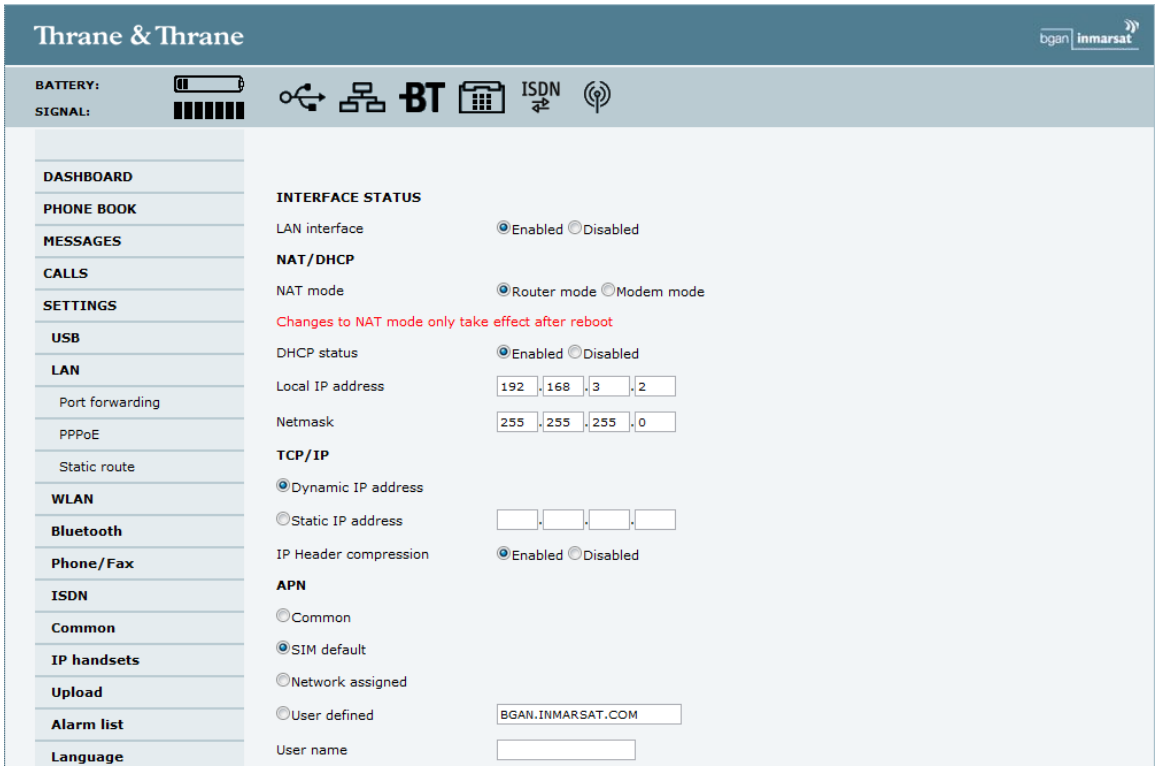

Figure 30 Thrane & Thrane Network Configuration Options

1. Normal BGAN Operations

We connected our virtual workstations directly to the Thrane & Thrane BGAN as shown in Figure 31. This allowed our queries and updates to be performed in a realistic manner. We performed the tests of Windows XP and Windows 7 manual and automatic updates. Since the virtual workstations were connected directly to the BGAN, the ability to capture packets and monitor

bandwidth usage was lost. However, we confirmed the Thrane & Thrane BGAN allowed normal updates to occur by monitoring successful installation of the updates.

Figure 31 Normal BGAN Operations

2. BGAN Operations with OpenDNS

To utilize OpenDNS, or any other custom DNS services, without manually configuring the workstation, an alternative DHCP server from the built in Thrane & Thrane BGAN DHCP server needed to be implemented. We recreated the test environment implemented in Experiments One and Two replacing our consumer ISP with a connection to the Thrane & Thrane BGAN as shown in Figure 32. The Tomato router was configured to utilize OpenDNS for queries and we ensured OpenDNS was not configured to block queries necessary for performing Windows Updates.

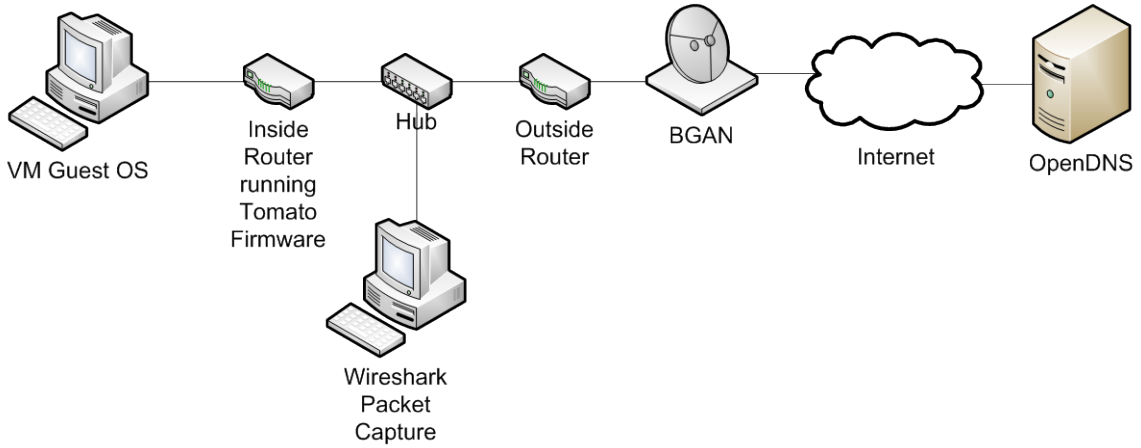

Figure 32 BGAN Experiments

We performed manual and automatic updates utilizing Windows XP and Windows 7. All update attempts completed normally as they had in Experiment One. The manual update of Windows XP is provided as an example. Utilizing a 485 KB update required 1,104.55 KB of bandwidth (791.99 KB received and 312.56 KB transmitted) as shown in Figure 33 with the packet capture displayed in Appendix D.

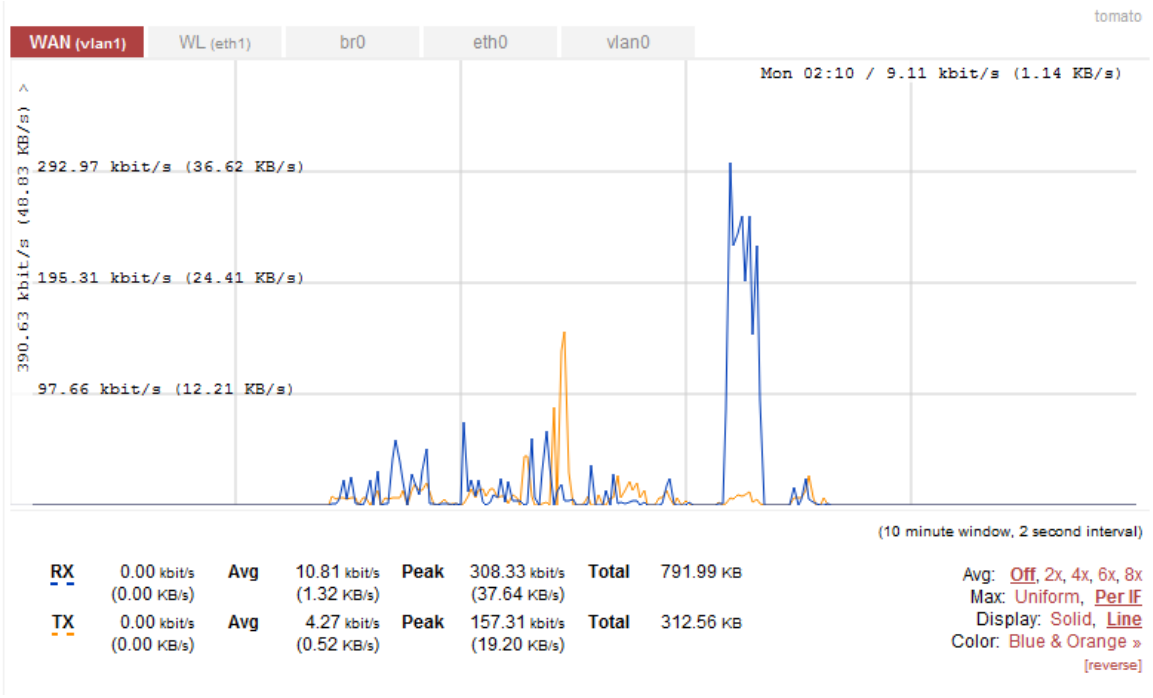

Figure 33 Normal Windows XP Manual Update through BGAN

3. BGAN Operations with DNS Tampering utilizing OpenDNS

We reconfigured the settings within OpenDNS as we had done in Experiment Two as shown in Figure 21 and ensured Tomato was configured to query OpenDNS. We attempted to perform manual and automatic updates for both Windows XP and Windows 7 as we had for our previous tests. These updates failed with the same results as Experiment Two.

We attempted to perform a manual update of Windows XP. The update process failed after utilizing 232.55 KB if bandwidth (175.63 KB received and 56.92 KB transmitted) as shown in Figure 34. The packet capture of the update process is shown in Appendix E, Annex 1.

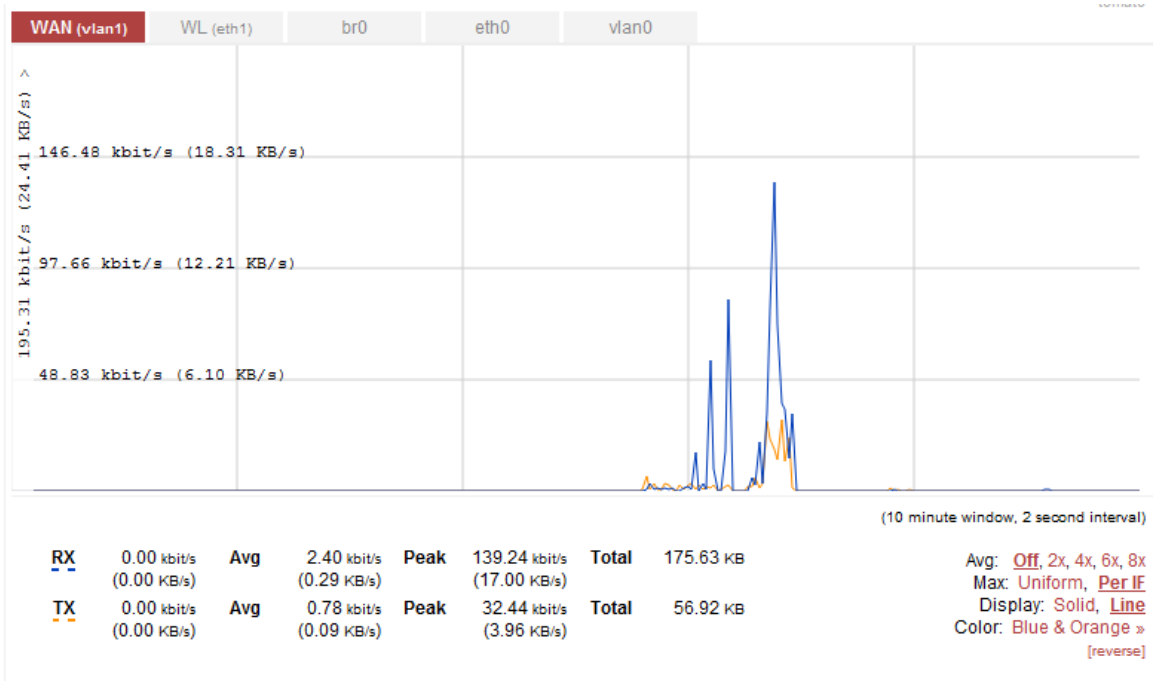

Figure 34 Blocked Windows XP Manual Update through BGAN

The automatic Windows XP update failed with similar results as the manual update. Figure 35 displays the update utilized 8.693 KB of bandwidth (4.088 KB received and 4.605 KB transmitted). The results of the packet capture are displayed in Appendix E Annex 2.

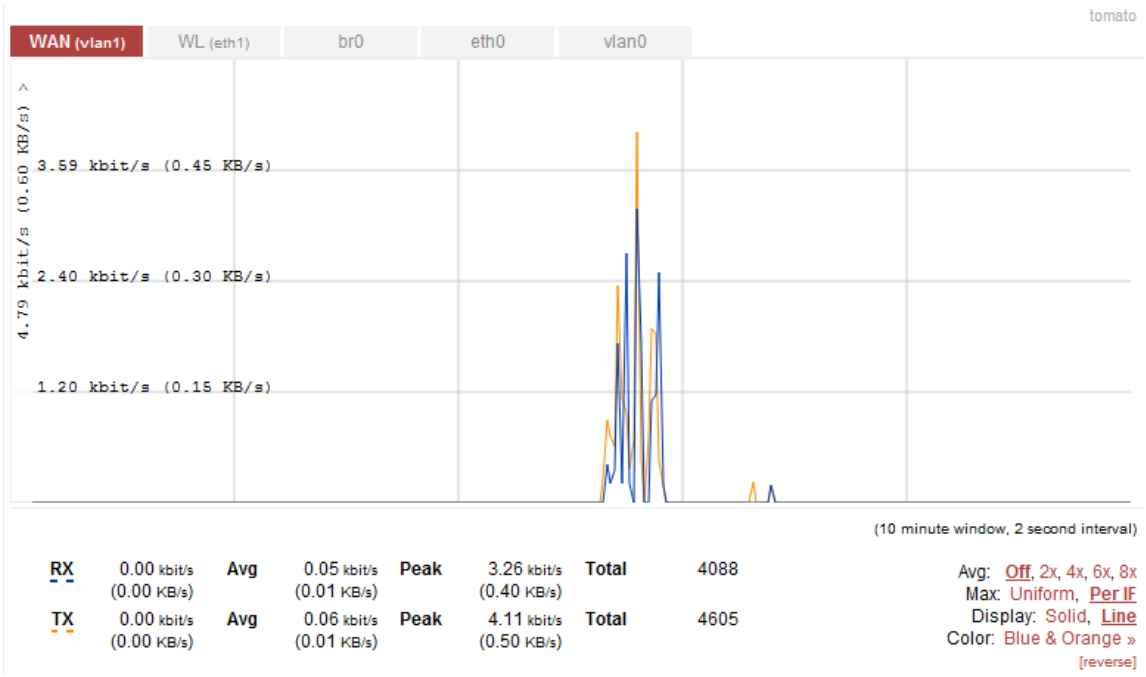

Figure 35 Blocked Windows XP Automatic Update through BGAN

Windows 7 manual update failed after utilizing 8.311 KB (4.487 KB received and 3.824 KB transmitted) of bandwidth as shown in Figure 36. The blocked update is shown through the packet capture displayed in Appendix E, Annex 3.

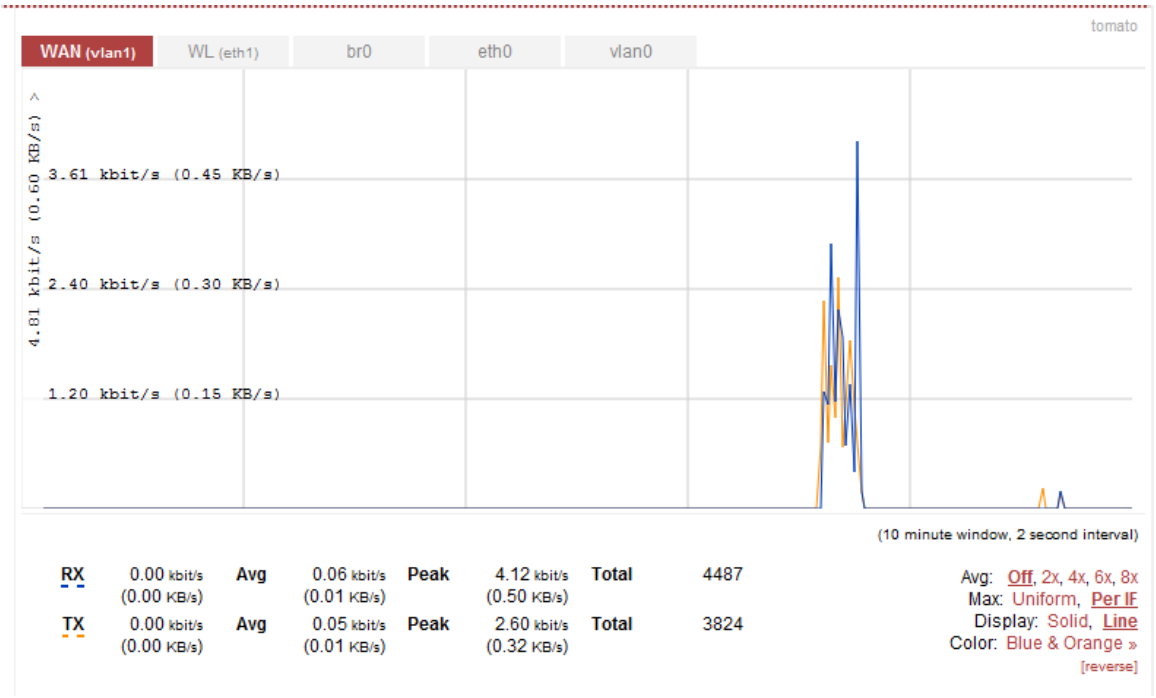

Figure 36 Blocked Windows 7 Manual Update through BGAN

Configuring Windows 7 to perform automatic updates failed after utilizing 9.779 KB of bandwidth (4.828 KB received and 4.951 KB transmitted) as shown in Figure 37. Appendix E, Annex 4 shows the updates were blocked.

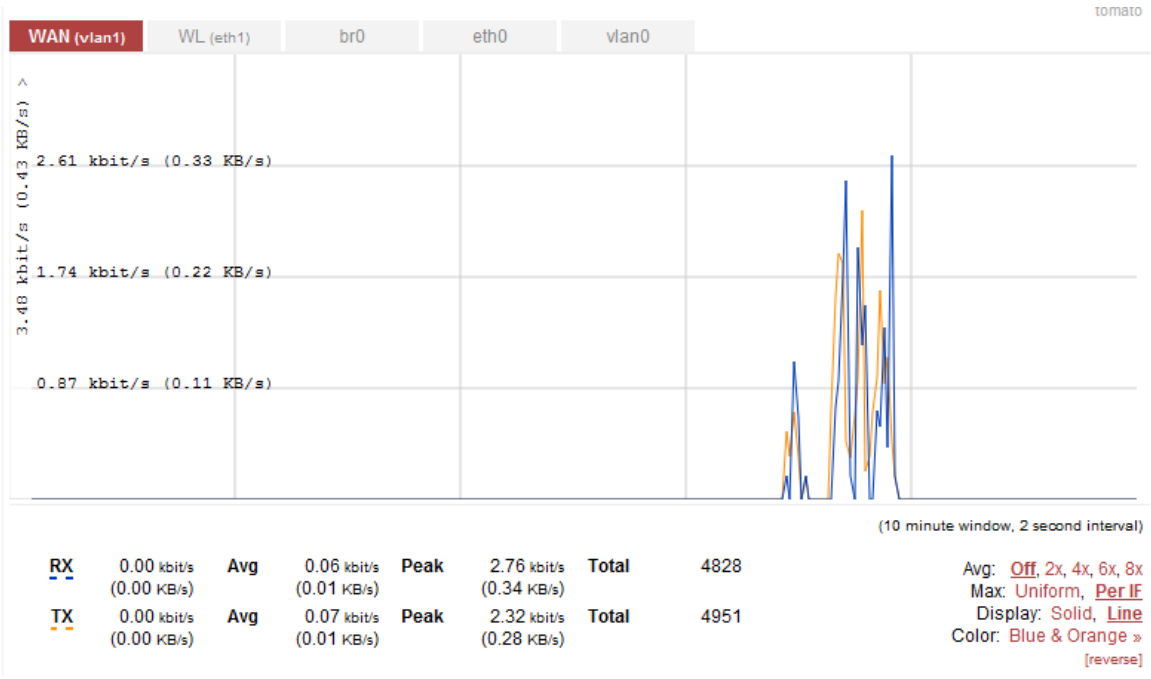

Figure 37 Blocked Windows 7 Automatic Update through BGAN

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSION

A. DISCUSSION

We evaluated DNS Tampering as a method of performing content filtering in low resource networks as a means to conserve bandwidth. We determined it is possible to utilize DNS Tampering to prevent both Windows XP and Windows 7 from performing updates to the operating system either automatically or manually.

Experiment One identified the DNS responses required by both operating systems in performing automatic and manual updates. The updates were initiated in a variety of methods to ensure the research encompassed virtually all possible instances. The specific, necessary DNS queries and responses were isolated and analyzed.

Experiment Two evaluated the effectiveness of DNS Tampering as a method to prevent both Windows XP and Windows 7 from performing updates. The tests were performed utilizing a consumer grade, commercial Internet provider.

Experiment Three evaluated equipment typically used in an HFN to evaluate the effectiveness of DNS Tampering as a method to prevent both Windows XP and Windows 7 from performing updates. The tests were performed utilizing a commercially available BGAN and showed DNS Tampering was an effective method for managing bandwidth in resource constrained networks.

We utilized a commercial DNS provider to control DNS Tampering for our experimentation. However, local resources and configurations could provide similar results.

The use of a commercial DNS provider, administrable via the web, allows remote management of the query filters. This alleviates the burden of requiring a network administrator to be present at the HFN for HA/DR. This method could

create an additional management issue of ensuring the DNS Tampering was implemented correctly and was operational. It provides the additional benefit of allowing remote administration without requiring access to the HFN network.

Utilizing local resources could alleviate the risk associated with a network configuration change rendering the solution inoperable. However, local management could create additional administration burdens and may require specialized or specific hardware and software.

DNS Tampering is an effective method for managing bandwidth in resource constrained networks and should be implemented within HFNs supporting HA/DR. The ability to limit access to specific resources on the Internet will reduce bandwidth requirements and costs associated with supporting HA/DR activities. Figure 38 shows a recommend solution for implementing DNS Tampering in resource constrained networks.

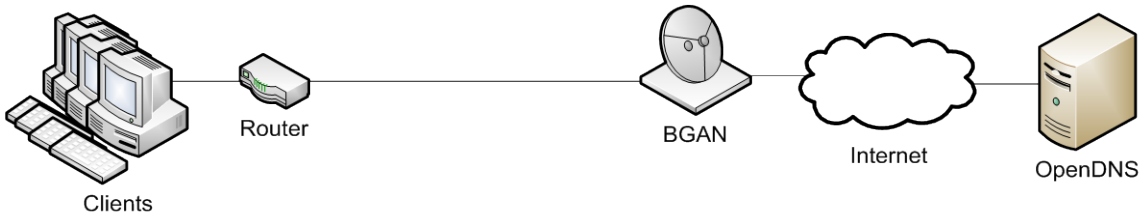

Figure 38 Recommended Solution

B. FUTURE RESEARCH

There are a number of areas for future research involving bandwidth management in resource constrained networks. This research only addressed a single application, Windows operating system updates, and single method, DNS Tampering. Additional operating systems, applications, and appliances should be analyzed and considered. Additional methods of managing bandwidth might also be explored and could naturally build upon these research findings.

This research focused on DNS Tampering as a method of content filtering to achieve bandwidth management. Other methods of content filtering as well as

alternative methods of managing bandwidth could be explored. Implementation of content filtering through a proxy server with caching capabilities could reduce bandwidth requirements. Research could explore implications associated with operating a proxy server within an HFN, as well as outside of, but accessible by, an HFN.

TCP/IP Content Filtering could to limit broad categories of traffic based on specific content. This could enable filtering of traffic based on type without explicit knowledge of specific applications to filter. Future research might also consider the effectiveness, as well as develop filtering rules, of TCP/IP Content Filtering for bandwidth management. While previous research discussed some of the implications generally associated with TCP/IP Header Filtering, the effectiveness and implications associated with HFNs could be evaluated.

Methods of bandwidth management other than content filtering could be explored. Quality of Service (QoS) could be evaluated as a method to control a variety of traffic regardless of source, destination, or specific application. Instead, quantity of sustained traffic could be used in determining filtering rules. Research could evaluate the impact and implications on end users associated with implementing QoS in resource constrained.

Cloud-based applications are becoming more prevalent for online data storage and backups. These applications have the potential to utilize vast amounts of bandwidth with little user interaction. Many applications rely on periodic updates for security and usability improvements, and frequently these updates are performed in the background. A study could produce a list of applications utilizing bandwidth in deployed HFNs and the ability to limit bandwidth consumption.

Alternative methods, including smart phones and tablets, of accessing information are becoming more prevalent. These appliances could introduce entirely new requirements and demands on bandwidth. Their use and impact on HFNs may also prove beneficial to this area of research.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A PACKET CAPTURE TESTING TOMATO INTERCEPTING DNS QUERIES

ANNEX 1 PACKET CAPTURE OF NORMAL DNS QUERY WITHOUT TOMATO INTERCEPTING DNS QUERIES

```
No.     Time        Source                Destination           Protocol Info
  22293 156338.804322 192.168.10.100        208.67.222.222        DNS      Standard query A google.com

User Datagram Protocol, Src Port: casp (1130), Dst Port: domain (53)
Domain Name System (query)
    Queries
        google.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  22294  156339.074404  208.67.222.222          192.168.10.100          DNS       Standard query response A
            74.125.224.41 A 74.125.224.37 A 74.125.224.32 A 74.125.224.34 A 74.125.224.35 A 74.125.224.33 A
            74.125.224.39 A 74.125.224.46 A 74.125.224.36 A 74.125.224.40 A 74.125.224.38

User Datagram Protocol, Src Port: domain (53), Dst Port: casp (1130)
Domain Name System (response)
    Queries
        google.com: type A, class IN
    Answers
        google.com: type A, class IN, addr 74.125.224.41
        google.com: type A, class IN, addr 74.125.224.37
        google.com: type A, class IN, addr 74.125.224.32
        google.com: type A, class IN, addr 74.125.224.34
        google.com: type A, class IN, addr 74.125.224.35
        google.com: type A, class IN, addr 74.125.224.33
        google.com: type A, class IN, addr 74.125.224.39
        google.com: type A, class IN, addr 74.125.224.46
        google.com: type A, class IN, addr 74.125.224.36
        google.com: type A, class IN, addr 74.125.224.40
        google.com: type A, class IN, addr 74.125.224.38
```

ANNEX 2 PACKET CAPTURE OF DNS QUERY OF BLOCKED DOMAIN WITHOUT TOMATO INTERCEPTING DNS QUERIES

```
No.     Time        Source                Destination           Protocol Info
    622 100.270608  192.168.10.100        208.67.222.222        DNS      Standard query A google.com

User Datagram Protocol, Src Port: eicon-x25 (1439), Dst Port: domain (53)
Domain Name System (query)
    Queries
        google.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
    623  100.567000   208.67.222.222           192.168.10.100          DNS        Standard query response A
            67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: eicon-x25 (1439)
Domain Name System (response)
    Queries
        google.com: type A, class IN
    Answers
        google.com: type A, class IN, addr 67.215.65.131
```

ANNEX 3 PACKET CAPTURE OF DNS QUERY OF BLOCKED DOMAIN TO ALTERNATIVE DNS SERVER WITHOUT TOMATO INTERCEPTING DNS QUERIES

```
No.     Time        Source                Destination           Protocol Info
   1872 5573.190395 192.168.10.100        4.2.2.1               DNS      Standard query A google.com

User Datagram Protocol, Src Port: stt (1607), Dst Port: domain (53)
Domain Name System (query)
    Queries
        google.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   1873  5573.436732  4.2.2.1                   192.168.10.100          DNS        Standard query response A
            173.194.38.174   A   173.194.38.160   A   173.194.38.161   A   173.194.38.162   A   173.194.38.163   A
```

```
            173.194.38.164  A  173.194.38.165  A  173.194.38.166  A  173.194.38.167  A  173.194.38.168  A
            173.194.38.169

User Datagram Protocol, Src Port: domain (53), Dst Port: stt (1607)
Domain Name System (response)
    Queries
        google.com: type A, class IN
    Answers
        google.com: type A, class IN, addr 173.194.38.174
        google.com: type A, class IN, addr 173.194.38.160
        google.com: type A, class IN, addr 173.194.38.161
        google.com: type A, class IN, addr 173.194.38.162
        google.com: type A, class IN, addr 173.194.38.163
        google.com: type A, class IN, addr 173.194.38.164
        google.com: type A, class IN, addr 173.194.38.165
        google.com: type A, class IN, addr 173.194.38.166
        google.com: type A, class IN, addr 173.194.38.167
        google.com: type A, class IN, addr 173.194.38.168
        google.com: type A, class IN, addr 173.194.38.169
```

ANNEX 4 PACKET CAPTURE OF DNS QUERY OF BLOCKED DOMAIN TO ALTERNATIVE DNS SERVER WITH TOMATO INTERCEPTING DNS QUERIES

```
No.     Time        Source                Destination           Protocol Info
   1928 6812.899003 192.168.10.100        208.67.222.222        DNS      Standard query A google.com

User Datagram Protocol, Src Port: 63154 (63154), Dst Port: domain (53)
Domain Name System (query)
    Queries
        google.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   1929  6813.190897  208.67.222.222           192.168.10.100           DNS        Standard query response A
            67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 63154 (63154)
Domain Name System (response)
```

```
Queries
    google.com: type A, class IN
Answers
    google.com: type A, class IN, addr 67.215.65.131
```

APPENDIX B PACKET CAPTURE OF NORMAL UPDATES

ANNEX 1 PACKET CAPTURE OF NORMAL WINDOWS XP MANUAL UPDATE

```
No.     Time        Source                Destination           Protocol Info
   5974  12183.997403  192.168.10.100             208.67.222.222             DNS          Standard  query  A
           windowsupdate.microsoft.com

User Datagram Protocol, Src Port: 13305 (13305), Dst Port: domain (53)
Domain Name System (query)
    Queries
        windowsupdate.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   5975 12184.073636 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           windowsupdate.microsoft.nsatc.net CNAME www.update.microsoft.com.nsatc.net A 65.55.184.152

User Datagram Protocol, Src Port: domain (53), Dst Port: 13305 (13305)
Domain Name System (response)
    Queries
        windowsupdate.microsoft.com: type A, class IN
    Answers
        windowsupdate.microsoft.com: type CNAME, class IN, cname windowsupdate.microsoft.nsatc.net
        windowsupdate.microsoft.nsatc.net: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.184.152

No.     Time        Source                Destination           Protocol Info
   6018  12186.529362  192.168.10.100             208.67.222.222             DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 12243 (12243), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN
```

```
No.     Time        Source                Destination           Protocol Info
   6019 12186.575457 208.67.222.222         192.168.10.100         DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.184.152

User Datagram Protocol, Src Port: domain (53), Dst Port: 12243 (12243)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.184.152

No.     Time        Source                Destination           Protocol Info
   6200  12192.753812  192.168.10.100             208.67.222.222             DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 39916 (39916), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6201 12192.810139 208.67.222.222         192.168.10.100         DNS       Standard query response CNAME
           download.windowsupdate.nsatc.net  CNAME  main.dl.wu.akadns.net  CNAME  dom.dl.wu.akadns.net  CNAME
           dl.wu.ms.edgesuite.net CNAME a26.ms.akamai.net A 128.241.220.82 A 128.241.220.90

User Datagram Protocol, Src Port: domain (53), Dst Port: 39916 (39916)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net: type CNAME, class IN, cname main.dl.wu.akadns.net
        main.dl.wu.akadns.net: type CNAME, class IN, cname dom.dl.wu.akadns.net
        dom.dl.wu.akadns.net: type CNAME, class IN, cname dl.wu.ms.edgesuite.net
        dl.wu.ms.edgesuite.net: type CNAME, class IN, cname a26.ms.akamai.net
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.82
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.90
```

```
No.     Time        Source                Destination           Protocol Info
   6255 12193.803705 192.168.10.100        208.67.222.222        DNS      Standard query A c.microsoft.com

User Datagram Protocol, Src Port: 44383 (44383), Dst Port: domain (53)
Domain Name System (query)
    Queries
        c.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6256 12193.850172 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            c.microsoft.akadns.net A 64.4.11.36

User Datagram Protocol, Src Port: domain (53), Dst Port: 44383 (44383)
Domain Name System (response)
    Queries
        c.microsoft.com: type A, class IN
    Answers
        c.microsoft.com: type CNAME, class IN, cname c.microsoft.akadns.net
        c.microsoft.akadns.net: type A, class IN, addr 64.4.11.36

No.     Time        Source                Destination           Protocol Info
   6405  12197.983359  192.168.10.100             208.67.222.222             DNS          Standard  query  A
            download.windowsupdate.com

User Datagram Protocol, Src Port: 6522 (6522), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6406 12198.077060 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net  CNAME  main.dl.wu.akadns.net  CNAME  dom.dl.wu.akadns.net  CNAME
            dl.wu.ms.edgesuite.net CNAME a26.ms.akamai.net A 128.241.220.90 A 128.241.220.82

User Datagram Protocol, Src Port: domain (53), Dst Port: 6522 (6522)
Domain Name System (response)
    Queries
```

```
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net: type CNAME, class IN, cname main.dl.wu.akadns.net
        main.dl.wu.akadns.net: type CNAME, class IN, cname dom.dl.wu.akadns.net
        dom.dl.wu.akadns.net: type CNAME, class IN, cname dl.wu.ms.edgesuite.net
        dl.wu.ms.edgesuite.net: type CNAME, class IN, cname a26.ms.akamai.net
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.90
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.82

No.     Time        Source                Destination           Protocol Info
   6413  12198.363587  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 47128 (47128), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6414 12198.442475 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.184.152

User Datagram Protocol, Src Port: domain (53), Dst Port: 47128 (47128)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.184.152
```

ANNEX 2 PACKET CAPTURE OF NORMAL WINDOWS XP AUTOMATIC UPDATE

```
No.     Time        Source                Destination           Protocol Info
   5138  9316.269958  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com
```

```
User Datagram Protocol, Src Port: 42106 (42106), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   5139 9316.439912 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
           download.windowsupdate.com.c.footprint.net A 8.27.252.253 A 8.27.236.252 A 8.27.254.249

User Datagram Protocol, Src Port: domain (53), Dst Port: 42106 (42106)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
            download.windowsupdate.com.fp.nsatc.net
        download.windowsupdate.com.fp.nsatc.net:       type        CNAME,        class        IN,        cname
            download.windowsupdate.com.c.footprint.net
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.252.253
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.236.252
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.254.249

No.     Time        Source                Destination           Protocol Info
   5147  9319.038757  192.168.10.100             208.67.222.222             DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 21295 (21295), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   5148 9319.203999 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.25.60

User Datagram Protocol, Src Port: domain (53), Dst Port: 21295 (21295)
```

```
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.25.60

No.     Time        Source                Destination           Protocol Info
   5381  9432.412066  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           au.download.windowsupdate.com

User Datagram Protocol, Src Port: 13320 (13320), Dst Port: domain (53)
Domain Name System (query)
    Queries
        au.download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   5382 9432.649175 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           audownload.windowsupdate.nsatc.net  CNAME  gfsaudownload.windowsupdate.nsatc.net  CNAME  mscom-au-
           any.vo.msecnd.net A 65.54.87.59 A 65.54.87.61

User Datagram Protocol, Src Port: domain (53), Dst Port: 13320 (13320)
Domain Name System (response)
    Queries
        au.download.windowsupdate.com: type A, class IN
    Answers
        au.download.windowsupdate.com: type CNAME, class IN, cname audownload.windowsupdate.nsatc.net
        audownload.windowsupdate.nsatc.net:        type        CNAME,        class        IN,        cname
            gfsaudownload.windowsupdate.nsatc.net
        gfsaudownload.windowsupdate.nsatc.net: type CNAME, class IN, cname mscom-au-any.vo.msecnd.net
        mscom-au-any.vo.msecnd.net: type A, class IN, addr 65.54.87.59
        mscom-au-any.vo.msecnd.net: type A, class IN, addr 65.54.87.61
```

ANNEX 3 PACKET CAPTURE OF NORMAL WINDOWS 7 MANUAL UPDATE

```
No.     Time        Source                Destination           Protocol Info
```

```
   1908  107.121645    192.168.10.100              208.67.222.222              DNS          Standard  query  A
            download.windowsupdate.com

User Datagram Protocol, Src Port: 39753 (39753), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   1909  107.138756   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net  CNAME  main.dl.wu.akadns.net  CNAME  dom.dl.wu.akadns.net  CNAME
            dl.wu.ms.edgesuite.net CNAME a26.ms.akamai.net A 128.241.220.90 A 128.241.220.82

User Datagram Protocol, Src Port: domain (53), Dst Port: 39753 (39753)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net: type CNAME, class IN, cname main.dl.wu.akadns.net
        main.dl.wu.akadns.net: type CNAME, class IN, cname dom.dl.wu.akadns.net
        dom.dl.wu.akadns.net: type CNAME, class IN, cname dl.wu.ms.edgesuite.net
        dl.wu.ms.edgesuite.net: type CNAME, class IN, cname a26.ms.akamai.net
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.90
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.82

No.     Time        Source                Destination           Protocol Info
   1910  107.144295    192.168.10.100              208.67.222.222              DNS          Standard  query  A
            download.windowsupdate.com

User Datagram Protocol, Src Port: 7386 (7386), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
   1911 107.160094   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net  CNAME  main.dl.wu.akadns.net  CNAME  dom.dl.wu.akadns.net  CNAME
            dl.wu.ms.edgesuite.net CNAME a26.ms.akamai.net A 128.241.220.90 A 128.241.220.82

User Datagram Protocol, Src Port: domain (53), Dst Port: 7386 (7386)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net: type CNAME, class IN, cname main.dl.wu.akadns.net
        main.dl.wu.akadns.net: type CNAME, class IN, cname dom.dl.wu.akadns.net
        dom.dl.wu.akadns.net: type CNAME, class IN, cname dl.wu.ms.edgesuite.net
        dl.wu.ms.edgesuite.net: type CNAME, class IN, cname a26.ms.akamai.net
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.90
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.82

No.     Time        Source                Destination           Protocol Info
   1921  110.253991   192.168.10.100             208.67.222.222             DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 5293 (5293), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   1922 110.265810   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            www.update.microsoft.com.nsatc.net A 65.55.200.139

User Datagram Protocol, Src Port: domain (53), Dst Port: 5293 (5293)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.200.139
```

```
No.     Time        Source                Destination           Protocol Info
   1923  110.272223   192.168.10.100             208.67.222.222             DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 34809 (34809), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   1924  110.288419   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.200.139

User Datagram Protocol, Src Port: domain (53), Dst Port: 34809 (34809)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.200.139

No.     Time        Source                Destination           Protocol Info
   1944  111.524969   192.168.10.100             208.67.222.222             DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 54584 (54584), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   1945  111.536643   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.200.139

User Datagram Protocol, Src Port: domain (53), Dst Port: 54584 (54584)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
```

```
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.200.139

No.     Time        Source                Destination           Protocol Info
   1946  111.542710   192.168.10.100             208.67.222.222             DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 43742 (43742), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   1947  111.557356   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.200.139

User Datagram Protocol, Src Port: domain (53), Dst Port: 43742 (43742)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.200.139
```

ANNEX 4 PACKET CAPTURE OF NORMAL WINDOWS 7 AUTOMATIC UPDATE

```
No.     Time        Source                Destination           Protocol Info
    333  111.971720   192.168.10.100             208.67.222.222             DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 37222 (37222), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
    334 111.984817   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net  CNAME  main.dl.wu.akadns.net  CNAME  dom.dl.wu.akadns.net  CNAME
            dl.wu.ms.edgesuite.net CNAME a26.ms.akamai.net A 128.241.220.90 A 128.241.220.82

User Datagram Protocol, Src Port: domain (53), Dst Port: 37222 (37222)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net: type CNAME, class IN, cname main.dl.wu.akadns.net
        main.dl.wu.akadns.net: type CNAME, class IN, cname dom.dl.wu.akadns.net
        dom.dl.wu.akadns.net: type CNAME, class IN, cname dl.wu.ms.edgesuite.net
        dl.wu.ms.edgesuite.net: type CNAME, class IN, cname a26.ms.akamai.net
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.90
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.82

No.     Time        Source                Destination           Protocol Info
    335  112.016044   192.168.10.100             208.67.222.222              DNS          Standard  query  A
            download.windowsupdate.com

User Datagram Protocol, Src Port: 37323 (37323), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
    336 112.032766   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net  CNAME  main.dl.wu.akadns.net  CNAME  dom.dl.wu.akadns.net  CNAME
            dl.wu.ms.edgesuite.net CNAME a26.ms.akamai.net A 128.241.220.90 A 128.241.220.82

User Datagram Protocol, Src Port: domain (53), Dst Port: 37323 (37323)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net: type CNAME, class IN, cname main.dl.wu.akadns.net
```

```
        main.dl.wu.akadns.net: type CNAME, class IN, cname dom.dl.wu.akadns.net
        dom.dl.wu.akadns.net: type CNAME, class IN, cname dl.wu.ms.edgesuite.net
        dl.wu.ms.edgesuite.net: type CNAME, class IN, cname a26.ms.akamai.net
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.90
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.82

No.     Time        Source                Destination           Protocol Info
    346  114.645173   192.168.10.100             208.67.222.222             DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 32239 (32239), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
    347  114.657401   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            www.update.microsoft.com.nsatc.net A 65.55.200.139

User Datagram Protocol, Src Port: domain (53), Dst Port: 32239 (32239)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.200.139

No.     Time        Source                Destination           Protocol Info
    348  114.664207   192.168.10.100             208.67.222.222             DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 26697 (26697), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
    349 114.680143   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            www.update.microsoft.com.nsatc.net A 65.55.200.139

User Datagram Protocol, Src Port: domain (53), Dst Port: 26697 (26697)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.200.139

No.     Time        Source                Destination           Protocol Info
    366  116.166580   192.168.10.100             208.67.222.222             DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 33871 (33871), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
    368 116.182296   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            www.update.microsoft.com.nsatc.net A 65.55.200.139

User Datagram Protocol, Src Port: domain (53), Dst Port: 33871 (33871)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.200.139

No.     Time        Source                Destination           Protocol Info
    369  116.190315   192.168.10.100             208.67.222.222             DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 60614 (60614), Dst Port: domain (53)
Domain Name System (query)
```

```
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
    370 116.200570   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            www.update.microsoft.com.nsatc.net A 65.55.200.139

User Datagram Protocol, Src Port: domain (53), Dst Port: 60614 (60614)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.200.139

No.     Time        Source                Destination           Protocol Info
   3920  170.073922   192.168.10.100             208.67.222.222              DNS          Standard  query  A
            www.download.windowsupdate.com

User Datagram Protocol, Src Port: 57022 (57022), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   3921 170.086143   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            www.download.windowsupdate.nsatc.net  CNAME  main.dl.wu.akadns.net  CNAME  dom.dl.wu.akadns.net
            CNAME dl.wu.ms.edgesuite.net CNAME a26.ms.akamai.net A 128.241.220.82 A 128.241.220.90

User Datagram Protocol, Src Port: domain (53), Dst Port: 57022 (57022)
Domain Name System (response)
    Queries
        www.download.windowsupdate.com: type A, class IN
    Answers
        www.download.windowsupdate.com: type CNAME, class IN, cname www.download.windowsupdate.nsatc.net
        www.download.windowsupdate.nsatc.net: type CNAME, class IN, cname main.dl.wu.akadns.net
        main.dl.wu.akadns.net: type CNAME, class IN, cname dom.dl.wu.akadns.net
        dom.dl.wu.akadns.net: type CNAME, class IN, cname dl.wu.ms.edgesuite.net
```

```
        dl.wu.ms.edgesuite.net: type CNAME, class IN, cname a26.ms.akamai.net
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.82
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.90

No.     Time        Source                Destination           Protocol Info
   3922  170.093560   192.168.10.100             208.67.222.222              DNS          Standard  query  A
            www.download.windowsupdate.com

User Datagram Protocol, Src Port: 60218 (60218), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   3923 170.108420   208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            www.download.windowsupdate.nsatc.net  CNAME  main.dl.wu.akadns.net  CNAME  dom.dl.wu.akadns.net
            CNAME dl.wu.ms.edgesuite.net CNAME a26.ms.akamai.net A 128.241.220.82 A 128.241.220.90

User Datagram Protocol, Src Port: domain (53), Dst Port: 60218 (60218)
Domain Name System (response)
    Queries
        www.download.windowsupdate.com: type A, class IN
    Answers
        www.download.windowsupdate.com: type CNAME, class IN, cname www.download.windowsupdate.nsatc.net
        www.download.windowsupdate.nsatc.net: type CNAME, class IN, cname main.dl.wu.akadns.net
        main.dl.wu.akadns.net: type CNAME, class IN, cname dom.dl.wu.akadns.net
        dom.dl.wu.akadns.net: type CNAME, class IN, cname dl.wu.ms.edgesuite.net
        dl.wu.ms.edgesuite.net: type CNAME, class IN, cname a26.ms.akamai.net
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.82
        a26.ms.akamai.net: type A, class IN, addr 128.241.220.90
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C PACKET CAPTURE OF BLOCKED UPDATES

ANNEX 1 PACKET CAPTURE OF BLOCKED WINDOWS XP MANUAL UPDATE

```
No.     Time        Source                Destination           Protocol Info
   5679  1654.498410  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           windowsupdate.microsoft.com

User Datagram Protocol, Src Port: 12469 (12469), Dst Port: domain (53)
Domain Name System (query)
    Queries
        windowsupdate.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   5680  1654.509912  208.67.222.222            192.168.10.100          DNS       Standard query response CNAME
           windowsupdate.microsoft.nsatc.net CNAME www.update.microsoft.com.nsatc.net A 65.55.184.152

User Datagram Protocol, Src Port: domain (53), Dst Port: 12469 (12469)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131
```

ANNEX 2 PACKET CAPTURE OF BLOCKED WINDOWS XP AUTOMATIC UPDATE

```
No.     Time        Source                Destination           Protocol Info
   6437  2435.599901  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 23267 (23267), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN
```

```
No.     Time        Source                Destination           Protocol Info
   6438 2435.612323 208.67.222.222           192.168.10.100           DNS        Standard query response A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 23267 (23267)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6454 2435.710788 192.168.10.100             208.67.222.222              DNS          Standard query A
           download.microsoft.com

User Datagram Protocol, Src Port: 31299 (31299), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6455 2435.722012 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.microsoft.com.nsatc.net CNAME main.dl.ms.akadns.net CNAME dom.dl.ms.akadns.net CNAME
           dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.88 A 128.241.220.87

User Datagram Protocol, Src Port: domain (53), Dst Port: 31299 (31299)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87
```

```
No.     Time        Source                Destination           Protocol Info
   6462  2435.786473  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 30743 (30743), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6463  2435.797749  208.67.222.222           192.168.10.100           DNS        Standard query response A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 30743 (30743)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131
```

ANNEX 3 PACKET CAPTURE OF BLOCKED WINDOWS 7 MANUAL UPDATE

```
No.     Time        Source                Destination           Protocol Info
   6495  3224.692137  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 60648 (60648), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6496  3224.703284  208.67.222.222           192.168.10.100           DNS        Standard query response A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 60648 (60648)
Domain Name System (response)
```

```
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6497  3224.709819  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 42227 (42227), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6498  3224.719094  208.67.222.222           192.168.10.100           DNS        Standard query response A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 42227 (42227)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6519  3225.209306  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.microsoft.com

User Datagram Protocol, Src Port: 15924 (15924), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6520  3225.219796  208.67.222.222           192.168.10.100          DNS       Standard query response CNAME
         download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
         dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.87 A 128.241.220.88
```

```
User Datagram Protocol, Src Port: domain (53), Dst Port: 15924 (15924)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88

No.     Time        Source                Destination           Protocol Info
   6521  3225.225174  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           download.microsoft.com

User Datagram Protocol, Src Port: 10168 (10168), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6522 3225.235758 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
           dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.87 A 128.241.220.88

User Datagram Protocol, Src Port: domain (53), Dst Port: 10168 (10168)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
```

```
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88

No.     Time        Source                Destination           Protocol Info
   6529  3225.313985  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 11748 (11748), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6530  3225.326185  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
            67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 11748 (11748)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6531  3225.332304  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 10706 (10706), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6532  3225.346376  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
            67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 10706 (10706)
Domain Name System (response)
```

```
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131
```

ANNEX 4 PACKET CAPTURE OF BLOCKED WINDOWS 7 AUTOMATIC UPDATE

```
No.     Time        Source                Destination           Protocol Info
   6565  3927.555658  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 16973 (16973), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6566  3927.566788  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 16973 (16973)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6567  3928.545605  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 23561 (23561), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
   6568  3928.555282  208.67.222.222           192.168.10.100           DNS        Standard query response A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 23561 (23561)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6569  3928.562920  192.168.10.100             208.67.222.222             DNS          Standard query A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 63193 (63193), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6570  3928.573296  208.67.222.222           192.168.10.100           DNS        Standard query response A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 63193 (63193)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6589  3931.250096  192.168.10.100             208.67.222.222             DNS          Standard query A
         download.microsoft.com

User Datagram Protocol, Src Port: 15752 (15752), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN
```

```
No.     Time        Source                Destination           Protocol Info
   6590 3931.266099 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
           dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.88 A 128.241.220.87

User Datagram Protocol, Src Port: domain (53), Dst Port: 15752 (15752)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87

No.     Time        Source                Destination           Protocol Info
   6591  3931.273650  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.microsoft.com

User Datagram Protocol, Src Port: 53054 (53054), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6592 3931.283577 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
           dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.88 A 128.241.220.87

User Datagram Protocol, Src Port: domain (53), Dst Port: 53054 (53054)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
```

```
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87

No.     Time        Source                Destination           Protocol Info
   6601  3933.923892  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 28476 (28476), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6602  3933.936890  208.67.222.222           192.168.10.100           DNS        Standard query response A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 28476 (28476)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6603  3933.947403  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 59848 (59848), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
   6604  3933.957206  208.67.222.222           192.168.10.100           DNS        Standard query response A
            67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 59848 (59848)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D PACKET CAPTURE OF NORMAL WINDOWS XP UPDATE THROUGH BGAN

```
No.     Time        Source                Destination           Protocol Info
  13978  7134.831460  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           windowsupdate.microsoft.com

User Datagram Protocol, Src Port: accel (4108), Dst Port: domain (53)
Domain Name System (query)
    Queries
        windowsupdate.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  13979  7135.825247  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           windowsupdate.microsoft.com

User Datagram Protocol, Src Port: accel (4108), Dst Port: domain (53)
Domain Name System (query)
    Queries
        windowsupdate.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  13980  7136.825406  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           windowsupdate.microsoft.com

User Datagram Protocol, Src Port: accel (4108), Dst Port: domain (53)
Domain Name System (query)
    Queries
        windowsupdate.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  13981 7136.850104 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           windowsupdate.microsoft.nsatc.net CNAME www.update.microsoft.com.nsatc.net A 65.55.184.152

User Datagram Protocol, Src Port: domain (53), Dst Port: accel (4108)
Domain Name System (response)
    Queries
```

```
        windowsupdate.microsoft.com: type A, class IN
    Answers
        windowsupdate.microsoft.com: type CNAME, class IN, cname windowsupdate.microsoft.nsatc.net
        windowsupdate.microsoft.nsatc.net: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.184.152

No.     Time        Source                Destination           Protocol Info
  13983 7137.090180 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           windowsupdate.microsoft.nsatc.net CNAME www.update.microsoft.com.nsatc.net A 65.55.184.152

User Datagram Protocol, Src Port: domain (53), Dst Port: accel (4108)
Domain Name System (response)
    Queries
        windowsupdate.microsoft.com: type A, class IN
    Answers
        windowsupdate.microsoft.com: type CNAME, class IN, cname windowsupdate.microsoft.nsatc.net
        windowsupdate.microsoft.nsatc.net: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.184.152

No.     Time        Source                Destination           Protocol Info
  13985 7137.650820 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           windowsupdate.microsoft.nsatc.net CNAME www.update.microsoft.com.nsatc.net A 65.55.184.152

User Datagram Protocol, Src Port: domain (53), Dst Port: accel (4108)
Domain Name System (response)
    Queries
        windowsupdate.microsoft.com: type A, class IN
    Answers
        windowsupdate.microsoft.com: type CNAME, class IN, cname windowsupdate.microsoft.nsatc.net
        windowsupdate.microsoft.nsatc.net: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.184.152

No.     Time        Source                Destination           Protocol Info
  14047  7152.280836  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 37447 (37447), Dst Port: domain (53)
Domain Name System (query)
```

```
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14049 7153.090444 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.13.91

User Datagram Protocol, Src Port: domain (53), Dst Port: 37447 (37447)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.13.91

No.     Time        Source                Destination           Protocol Info
  14274  7192.319586  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 24974 (24974), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14275  7193.313054  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 24974 (24974), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14276  7194.310142  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 24974 (24974), Dst Port: domain (53)
```

```
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14277 7194.520538 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
            download.windowsupdate.com.c.footprint.net A 8.26.199.124 A 8.27.236.252 A 8.27.254.126

User Datagram Protocol, Src Port: domain (53), Dst Port: 24974 (24974)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
            download.windowsupdate.com.fp.nsatc.net
        download.windowsupdate.com.fp.nsatc.net:       type        CNAME,        class        IN,        cname
            download.windowsupdate.com.c.footprint.net
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.26.199.124
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.236.252
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.254.126

No.     Time        Source                Destination           Protocol Info
  14279 7195.160722 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
            download.windowsupdate.com.c.footprint.net A 8.27.236.252 A 8.27.254.126 A 8.26.199.124

User Datagram Protocol, Src Port: domain (53), Dst Port: 24974 (24974)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
            download.windowsupdate.com.fp.nsatc.net
        download.windowsupdate.com.fp.nsatc.net:       type        CNAME,        class        IN,        cname
            download.windowsupdate.com.c.footprint.net
```

```
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.236.252
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.254.126
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.26.199.124

No.     Time        Source                Destination           Protocol Info
  14344 7209.098183 192.168.10.100        208.67.222.222        DNS      Standard query A c.microsoft.com

User Datagram Protocol, Src Port: 16428 (16428), Dst Port: domain (53)
Domain Name System (query)
    Queries
        c.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14346 7210.090255 192.168.10.100        208.67.222.222        DNS      Standard query A c.microsoft.com

User Datagram Protocol, Src Port: 16428 (16428), Dst Port: domain (53)
Domain Name System (query)
    Queries
        c.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14348 7210.669419 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           c.microsoft.akadns.net A 64.4.11.36

User Datagram Protocol, Src Port: domain (53), Dst Port: 16428 (16428)
Domain Name System (response)
    Queries
        c.microsoft.com: type A, class IN
    Answers
        c.microsoft.com: type CNAME, class IN, cname c.microsoft.akadns.net
        c.microsoft.akadns.net: type A, class IN, addr 64.4.11.36

No.     Time        Source                Destination           Protocol Info
  14360 7210.919684 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           c.microsoft.akadns.net A 64.4.11.36

User Datagram Protocol, Src Port: domain (53), Dst Port: 16428 (16428)
Domain Name System (response)
```

```
    Queries
        c.microsoft.com: type A, class IN
    Answers
        c.microsoft.com: type CNAME, class IN, cname c.microsoft.akadns.net
        c.microsoft.akadns.net: type A, class IN, addr 64.4.11.36

No.     Time        Source                Destination           Protocol Info
  14419  7219.650206  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 62595 (62595), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14423  7220.636956  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 62595 (62595), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14425 7221.240664 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
           download.windowsupdate.com.c.footprint.net A 8.27.254.126 A 8.26.199.124 A 8.27.236.252

User Datagram Protocol, Src Port: domain (53), Dst Port: 62595 (62595)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
           download.windowsupdate.com.fp.nsatc.net
```

```
        download.windowsupdate.com.fp.nsatc.net:       type       CNAME,       class       IN,       cname
            download.windowsupdate.com.c.footprint.net
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.254.126
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.26.199.124
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.236.252

No.     Time        Source                Destination           Protocol Info
  14435 7221.480555 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
            download.windowsupdate.com.c.footprint.net A 8.26.199.124 A 8.27.236.252 A 8.27.254.126

User Datagram Protocol, Src Port: domain (53), Dst Port: 62595 (62595)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
            download.windowsupdate.com.fp.nsatc.net
        download.windowsupdate.com.fp.nsatc.net:       type       CNAME,       class       IN,       cname
            download.windowsupdate.com.c.footprint.net
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.26.199.124
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.236.252
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.254.126

No.     Time        Source                Destination           Protocol Info
  14478  7227.308296  192.168.10.100             208.67.222.222             DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 7060 (7060), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14480  7228.293830  192.168.10.100             208.67.222.222             DNS          Standard  query  A
            www.update.microsoft.com
```

```
User Datagram Protocol, Src Port: 7060 (7060), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14483 7228.759803 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.13.91

User Datagram Protocol, Src Port: domain (53), Dst Port: 7060 (7060)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.13.91

No.     Time        Source                Destination           Protocol Info
  14487 7229.240122 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           www.update.microsoft.com.nsatc.net A 65.55.13.91

User Datagram Protocol, Src Port: domain (53), Dst Port: 7060 (7060)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type CNAME, class IN, cname www.update.microsoft.com.nsatc.net
        www.update.microsoft.com.nsatc.net: type A, class IN, addr 65.55.13.91

No.     Time        Source                Destination           Protocol Info
  14584  7245.637303  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 58092 (58092), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN
```

```
No.     Time        Source                Destination           Protocol Info
  14585 7246.440685 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
            download.windowsupdate.com.c.footprint.net A 8.27.236.252 A 8.27.254.126 A 8.26.199.124

User Datagram Protocol, Src Port: domain (53), Dst Port: 58092 (58092)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
            download.windowsupdate.com.fp.nsatc.net
        download.windowsupdate.com.fp.nsatc.net:       type        CNAME,        class        IN,        cname
            download.windowsupdate.com.c.footprint.net
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.236.252
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.254.126
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.26.199.124

No.     Time        Source                Destination           Protocol Info
  14783  7268.146655  192.168.10.100             208.67.222.222              DNS          Standard  query  A
            download.windowsupdate.com

User Datagram Protocol, Src Port: 55300 (55300), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14784  7269.137447  192.168.10.100             208.67.222.222              DNS          Standard  query  A
            download.windowsupdate.com

User Datagram Protocol, Src Port: 55300 (55300), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
  14787  7270.151374  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 55300 (55300), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  14788 7271.000592 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
           download.windowsupdate.com.c.footprint.net A 8.27.236.252 A 8.27.254.126 A 8.26.199.124

User Datagram Protocol, Src Port: domain (53), Dst Port: 55300 (55300)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
            download.windowsupdate.com.fp.nsatc.net
        download.windowsupdate.com.fp.nsatc.net:       type       CNAME,       class       IN,       cname
            download.windowsupdate.com.c.footprint.net
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.236.252
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.254.126
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.26.199.124

No.     Time        Source                Destination           Protocol Info
  15028  7337.404522  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 5665 (5665), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
  15029  7338.402480  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 5665 (5665), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  15030  7339.415154  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 5665 (5665), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  15031  7341.402650  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 5665 (5665), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
  15032 7342.600373 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
           download.windowsupdate.com.c.footprint.net A 8.27.255.254 A 8.26.198.253 A 209.84.13.118

User Datagram Protocol, Src Port: domain (53), Dst Port: 5665 (5665)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
```

```
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
            download.windowsupdate.com.fp.nsatc.net
        download.windowsupdate.com.fp.nsatc.net:       type        CNAME,        class        IN,        cname
            download.windowsupdate.com.c.footprint.net
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.255.254
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.26.198.253
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 209.84.13.118

No.     Time        Source                Destination           Protocol Info
  15034 7343.400293 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.windowsupdate.nsatc.net     CNAME     download.windowsupdate.com.fp.nsatc.net     CNAME
            download.windowsupdate.com.c.footprint.net A 8.26.198.253 A 209.84.13.118 A 8.27.255.254

User Datagram Protocol, Src Port: domain (53), Dst Port: 5665 (5665)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type CNAME, class IN, cname download.windowsupdate.nsatc.net
        download.windowsupdate.nsatc.net:         type         CNAME,         class         IN,         cname
            download.windowsupdate.com.fp.nsatc.net
        download.windowsupdate.com.fp.nsatc.net:       type        CNAME,        class        IN,        cname
            download.windowsupdate.com.c.footprint.net
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.26.198.253
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 209.84.13.118
        download.windowsupdate.com.c.footprint.net: type A, class IN, addr 8.27.255.254
```

APPENDIX E PACKET CAPTURE OF BLOCKED UPDATES THROUGH BGAN

ANNEX 1 PACKET CAPTURE OF BLOCKED WINDOWS XP MANUAL UPDATE THROUGH BGAN

```
No.     Time        Source                Destination           Protocol Info
   6916  2013.173592  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           windowsupdate.microsoft.com

User Datagram Protocol, Src Port: 64290 (64290), Dst Port: domain (53)
Domain Name System (query)
    Queries
        windowsupdate.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6917  2014.175565  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           windowsupdate.microsoft.com

User Datagram Protocol, Src Port: 64290 (64290), Dst Port: domain (53)
Domain Name System (query)
    Queries
        windowsupdate.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6918  2015.168163  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           windowsupdate.microsoft.com

User Datagram Protocol, Src Port: 64290 (64290), Dst Port: domain (53)
Domain Name System (query)
    Queries
        windowsupdate.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   6919  2015.204442  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
           67.215.65.131
```

```
User Datagram Protocol, Src Port: domain (53), Dst Port: 64290 (64290)
Domain Name System (response)
    Queries
        windowsupdate.microsoft.com: type A, class IN
    Answers
        windowsupdate.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6921  2015.924001  208.67.222.222           192.168.10.100           DNS        Standard query response A
          67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 64290 (64290)
Domain Name System (response)
    Queries
        windowsupdate.microsoft.com: type A, class IN
    Answers
        windowsupdate.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   6923  2016.084047  208.67.222.222           192.168.10.100           DNS        Standard query response A
          67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 64290 (64290)
Domain Name System (response)
    Queries
        windowsupdate.microsoft.com: type A, class IN
    Answers
        windowsupdate.microsoft.com: type A, class IN, addr 67.215.65.131
```

ANNEX 2 PACKET CAPTURE OF BLOCKED WINDOWS XP AUTOMATIC UPDATE THROUGH BGAN

```
No.     Time        Source                Destination           Protocol Info
   7723  2795.014321  192.168.10.100              208.67.222.222              DNS          Standard query A
          download.windowsupdate.com

User Datagram Protocol, Src Port: 62411 (62411), Dst Port: domain (53)
Domain Name System (query)
```

```
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7724  2796.008103  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 62411 (62411), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7725  2796.981416  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 62411 (62411)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7727  2797.701355  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 62411 (62411)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7751  2805.357311  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.microsoft.com
```

```
User Datagram Protocol, Src Port: 43374 (43374), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7752  2806.351373  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.microsoft.com

User Datagram Protocol, Src Port: 43374 (43374), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7753  2807.351600  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.microsoft.com

User Datagram Protocol, Src Port: 43374 (43374), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7754 2807.421984 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
           dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.87 A 128.241.220.88

User Datagram Protocol, Src Port: domain (53), Dst Port: 43374 (43374)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
```

```
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88

No.     Time        Source                Destination           Protocol Info
   7756 2808.062020 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
            dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.87 A 128.241.220.88

User Datagram Protocol, Src Port: domain (53), Dst Port: 43374 (43374)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88

No.     Time        Source                Destination           Protocol Info
   7758 2808.222090 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
            dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.88 A 128.241.220.87

User Datagram Protocol, Src Port: domain (53), Dst Port: 43374 (43374)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87
```

```
No.     Time        Source                Destination           Protocol Info
   7768  2813.181400  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 59110 (59110), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7769  2814.148555  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 59110 (59110), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7770  2815.141424  208.67.222.222           192.168.10.100           DNS        Standard query response A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 59110 (59110)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7772  2815.621183  208.67.222.222           192.168.10.100           DNS        Standard query response A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 59110 (59110)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
```

```
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131
```

ANNEX 3 PACKET CAPTURE OF BLOCKED WINDOWS 7 MANUAL UPDATE THROUGH BGAN

```
No.     Time        Source                Destination           Protocol Info
   7810  3939.974114  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 13013 (13013), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7811  3940.971785  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 13013 (13013), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7812  3941.357727  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 13013 (13013)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7813  3941.367364  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.windowsupdate.com
```

```
User Datagram Protocol, Src Port: 40691 (40691), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7814 3942.157703 208.67.222.222           192.168.10.100           DNS        Standard query response A
          67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 13013 (13013)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7816 3942.237643 208.67.222.222           192.168.10.100           DNS        Standard query response A
          67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 40691 (40691)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7836 3947.366962 192.168.10.100              208.67.222.222              DNS          Standard query A
          download.microsoft.com

User Datagram Protocol, Src Port: 13661 (13661), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
   7838  3948.361931  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            download.microsoft.com

User Datagram Protocol, Src Port: 13661 (13661), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7839 3948.478910 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
            dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.87 A 128.241.220.88

User Datagram Protocol, Src Port: domain (53), Dst Port: 13661 (13661)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88

No.     Time        Source                Destination           Protocol Info
   7840  3948.486785  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            download.microsoft.com

User Datagram Protocol, Src Port: 47991 (47991), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
```

```
   7841 3949.358472 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
            dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.88 A 128.241.220.87

User Datagram Protocol, Src Port: domain (53), Dst Port: 13661 (13661)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87

No.     Time        Source                Destination           Protocol Info
   7843 3949.397639 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
            dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.88 A 128.241.220.87

User Datagram Protocol, Src Port: domain (53), Dst Port: 47991 (47991)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87

No.     Time        Source                Destination           Protocol Info
   7850  3951.888077  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            www.update.microsoft.com
```

```
User Datagram Protocol, Src Port: 59627 (59627), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7851 3952.717683 208.67.222.222           192.168.10.100           DNS        Standard query response A
            67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 59627 (59627)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7852  3952.726154  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 12212 (12212), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7853  3953.721492  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 12212 (12212), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7854 3953.837587 208.67.222.222           192.168.10.100           DNS        Standard query response A
            67.215.65.131
```

```
User Datagram Protocol, Src Port: domain (53), Dst Port: 12212 (12212)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7856  3954.957641  208.67.222.222           192.168.10.100           DNS        Standard query response A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 12212 (12212)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131
```

ANNEX 4 PACKET CAPTURE OF BLOCKED WINDOWS 7 AUTOMATIC UPDATE THROUGH BGAN

```
No.     Time        Source                Destination           Protocol Info
   7898  4591.931004  192.168.10.100             208.67.222.222             DNS          Standard query A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 49462 (49462), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7899  4592.932935  192.168.10.100             208.67.222.222             DNS          Standard query A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 49462 (49462), Dst Port: domain (53)
Domain Name System (query)
    Queries
```

```
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7900  4593.931156  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 49462 (49462), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7901  4594.244967  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 49462 (49462)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7902  4594.254525  192.168.10.100             208.67.222.222              DNS          Standard  query  A
           download.windowsupdate.com

User Datagram Protocol, Src Port: 62370 (62370), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7903  4594.964859  208.67.222.222           192.168.10.100           DNS        Standard  query  response  A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 49462 (49462)
Domain Name System (response)
    Queries
```

```
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7905  4595.256329  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.windowsupdate.com

User Datagram Protocol, Src Port: 62370 (62370), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.windowsupdate.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7906  4595.364865 208.67.222.222           192.168.10.100           DNS        Standard query response A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 62370 (62370)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7908  4596.724985 208.67.222.222           192.168.10.100           DNS        Standard query response A
         67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 62370 (62370)
Domain Name System (response)
    Queries
        download.windowsupdate.com: type A, class IN
    Answers
        download.windowsupdate.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7930  4603.106001  192.168.10.100             208.67.222.222              DNS          Standard  query  A
         download.microsoft.com
```

```
User Datagram Protocol, Src Port: 25659 (25659), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7931  4604.103399  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.microsoft.com

User Datagram Protocol, Src Port: 25659 (25659), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7932  4605.112278  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           download.microsoft.com

User Datagram Protocol, Src Port: 25659 (25659), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7933 4606.095322 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
           download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
           dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.88 A 128.241.220.87

User Datagram Protocol, Src Port: domain (53), Dst Port: 25659 (25659)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
```

```
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87

No.     Time        Source                Destination           Protocol Info
   7934  4606.109701  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            download.microsoft.com

User Datagram Protocol, Src Port: 33721 (33721), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7935  4607.103277  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            download.microsoft.com

User Datagram Protocol, Src Port: 33721 (33721), Dst Port: domain (53)
Domain Name System (query)
    Queries
        download.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7936 4607.295765 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
            dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.87 A 128.241.220.88

User Datagram Protocol, Src Port: domain (53), Dst Port: 33721 (33721)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87
```

```
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88

No.     Time        Source                Destination           Protocol Info
   7938 4608.335833 208.67.222.222          192.168.10.100          DNS       Standard query response CNAME
            download.microsoft.com.nsatc.net  CNAME  main.dl.ms.akadns.net  CNAME  dom.dl.ms.akadns.net  CNAME
            dl.ms.d4p.net CNAME a767.ms.akamai.net A 128.241.220.88 A 128.241.220.87

User Datagram Protocol, Src Port: domain (53), Dst Port: 33721 (33721)
Domain Name System (response)
    Queries
        download.microsoft.com: type A, class IN
    Answers
        download.microsoft.com: type CNAME, class IN, cname download.microsoft.com.nsatc.net
        download.microsoft.com.nsatc.net: type CNAME, class IN, cname main.dl.ms.akadns.net
        main.dl.ms.akadns.net: type CNAME, class IN, cname dom.dl.ms.akadns.net
        dom.dl.ms.akadns.net: type CNAME, class IN, cname dl.ms.d4p.net
        dl.ms.d4p.net: type CNAME, class IN, cname a767.ms.akamai.net
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.88
        a767.ms.akamai.net: type A, class IN, addr 128.241.220.87

No.     Time        Source                Destination           Protocol Info
   7946  4612.858839  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 53932 (53932), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7947  4613.854315  192.168.10.100              208.67.222.222              DNS          Standard  query  A
            www.update.microsoft.com

User Datagram Protocol, Src Port: 53932 (53932), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN
```

```
No.     Time        Source                Destination           Protocol Info
   7948  4614.853762  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 53932 (53932), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7949  4615.924902  208.67.222.222           192.168.10.100           DNS        Standard query response A
           67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 53932 (53932)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7950  4615.933051  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 37471 (37471), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN

No.     Time        Source                Destination           Protocol Info
   7951  4616.932723  192.168.10.100              208.67.222.222              DNS          Standard  query  A
           www.update.microsoft.com

User Datagram Protocol, Src Port: 37471 (37471), Dst Port: domain (53)
Domain Name System (query)
    Queries
        www.update.microsoft.com: type A, class IN
```

```
No.     Time        Source                Destination           Protocol Info
   7952  4617.204933  208.67.222.222           192.168.10.100           DNS        Standard query response A
            67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 37471 (37471)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131

No.     Time        Source                Destination           Protocol Info
   7954  4618.245473  208.67.222.222           192.168.10.100           DNS        Standard query response A
            67.215.65.131

User Datagram Protocol, Src Port: domain (53), Dst Port: 37471 (37471)
Domain Name System (response)
    Queries
        www.update.microsoft.com: type A, class IN
    Answers
        www.update.microsoft.com: type A, class IN, addr 67.215.65.131
```

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alexander, S., & Droms, R. (1997, March). RFC 2132: DHCP options and BOOTP vendor extensions. Retrieved January 3, 2012, from The Internet Engineering Task Force (IETF): http://tools.ietf.org/html/rfc2132

Dean, T. (2009). *Network+ guide to networks.* Boston: Course Technology.

Ding, C., Chi, C.-H., Deng, J., & Dong, C.-L. (1999). Centralized content-based web filtering and blocking: How far can it go? *Proceeding of IEEE International Conference on Systems, Man and Cybernetics (SMC)*, 2, (pp. 115 - 119). Tokyo.

Edelman, B. (2003, February). Websites sharing IP addresses: Prevalence and significance. Retrieved December 23, 2011, from Berkman Center for Internet & Society: http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/

Faris, R., & Villeneuve, N. (2008). Measuring global Internet filtering. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 5–28). Cambridge: MIT Press.

Hotel Internet Services (HIS). (2011). Retrieved December 8, 2011, from Hotel Internet Services (HIS): http://www.hotelwifi.com

Inmarsat. (2012). BGAN - Gloabal voice and broadband data. Retrieved Janaury 2, 2012, from Inmarsat: http://www.inmarsat.com/Services/Land/Services/High_speed_data/default.aspx

Kelley, S. (2011, February 18). DNSMASQ man page. Retrieved December 5, 2011, from www.thekelleys.org.uk: http://www.thekelleys.org.uk/dnsmasq/docs/dnsmasq-man.html

Kurose, J. F., & Ross, K. W. (2009). *Computer networking: A top-down approach.* New York: Addison-Wesley.

Luotonen, A., & Altis, K. (1994, November). World-wide web proxies. *Computer Networks and ISDN Systems*, 27(2), pp. 147–154.

Microsoft. (2007, October 12). How to disable client-side DNS caching in Windows XP and Windows Server 2003. Retrieved August 18, 2011, from Microsoft support: http://support.microsoft.com/kb/318803

Mockapetris, P. (1987, Novembera). RFC 1034: Domain names - Concepts and facilities. Retrieved January 3, 2012, from The Internet Engineering Task Force (IETF): http://tools.ietf.org/html/rfc1034

Mockapetris, P. (1987, Novemberb). RFC 1035: Domain names - Implementation and specification. Retrieved January 3, 2012, from The Internet Engineering Task Force (IETF): http://tools.ietf.org/html/rfc1035

Murdoch, S. J., & Anderson, R. (2008). Tools and technology of Internet filtering. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 57–72). Cambridge: MIT Press.

National Climatic Data Center. (2005, December 29). Hurricane Katrina. Retrieved November 8, 2011, from National Oceanic and Atmospheric Administration: http://www.ncdc.noaa.gov/special-reports/katrina.html

Naval Postgraduate School and the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD-NII). (2011). Katrina HFN timeline. Retrieved October 14, 2011, from Hastily Formed Networks for Humanitarian Assistance/Disaster Relief: http://faculty.nps.edu/dl/HFN/timeline1/HFN_Timeline1.html

Nelson, C. B., Steckler, B. D., & Stamberger, J. A. (2011). The evolution of Hastily Formed Networks for disaster response: Technologies, case dtudies, and future trends. Global Humanitarian Technology Conference (GHTC), 467–475. Retrieved from Cisco.

OpenDNS. (2011). OpenDNS. Retrieved August 6, 2011, from OpenDNS: http://www.opendns.com

SatCom Global. (2012, January 26). GS-35F-0337P General Services Administration federal supply service satellite commuinications equipment & service schedule pricelist. Chandler, Arizona.

Socolofsky, T., & Kale, C. (1991, January). RFC 1180: A TCP/IP tutorial. Retrieved August 17, 2011, from The Internet Engineering Task Force (IETF): http://tools.ietf.org/html/rfc1180

Steckler, B. (2010, September 8). Haiti earthquate after action report and lessons learned. Monterey, California.

W3Schools. (2012). OS platform statistics. Retrieved January 04, 2012, from W3Schools: http://www.w3schools.com/browsers/browsers_os.asp

Wireshark. (2008, April 12). Domain name system (DNS). Retrieved November 5, 2011, from Wireshark: http://wiki.wireshark.org/DNS

Zarate, J. (2011). Tomato firmware. Retrieved August 05, 2011, from Polar Cloud: http://www.polarcloud.com/tomato

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. William Welch
   Naval Postgraduate School
   Monterey, California

4. Dr. Doug MacKinnon
   Naval Postgraduate School
   Monterey, California

5. Director, NPS HFN
   Brian Steckler
   Naval Postgraduate School
   Monterey, California

6. Chair, Department of Information Sciences
   Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California